SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 16 February 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-46250	An issue in SOA2Login::commented of ScratchOAuth2 before commit a91879bd58fa83b09283c0708a1864cdf067c64a allows attackers to authenticate as other users on downstream components that rely on ScratchOAuth2.	10.0	More Details
CVE-2022-20699	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20749	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-20712	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-20711	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-20710	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-20709	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20707	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-20706	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-20705	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-20704	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-20703	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20702	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-20701	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-20700	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-20708	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an attacker to do any of the following: Execute arbitrary code Elevate privileges Execute arbitrary commands Bypass authentication and authorization protections Fetch and run unsigned software Cause denial of service (DoS) For more information about these vulnerabilities, see the Details section of this advisory.	10.0	More Details
CVE-2022-22536	SAP NetWeaver Application Server ABAP, SAP NetWeaver Application Server Java, ABAP Platform, SAP Content Server 7.53 and SAP Web Dispatcher are vulnerable for request smuggling and request concatenation. An unauthenticated attacker can prepend a victim's request with arbitrary data. This way, the attacker can execute functions impersonating the victim or poison intermediary Web caches. A successful attack could result in complete compromise of Confidentiality, Integrity and Availability of the system.	10.0	More Details
CVE-2021-42940	A Cross Site Scripting (XSS) vulnerability exists in Projeqtor 9.3.1 via /projeqtor/tool/saveAttachment.php, which allows an attacker to upload a SVG file containing malicious JavaScript code.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36302	All Dell EMC Integrated System for Microsoft Azure Stack Hub versions contain a privilege escalation vulnerability. A remote malicious user with standard level JEA credentials may potentially exploit this vulnerability to elevate privileges and take over the system.	9.9	More Details
CVE-2022-23992	XCOM Data Transport for Windows, Linux, and UNIX 11.6 releases contain a vulnerability due to insufficient input validation that could potentially allow remote attackers to execute arbitrary commands with elevated privileges.	9.8	More Details
CVE-2022-23389	PublicCMS v4.0 was discovered to contain a remote code execution (RCE) vulnerability via the cmdarray parameter.	9.8	More Details
CVE-2022-23337	DedeCMS v5.7.87 was discovered to contain a SQL injection vulnerability in article_coonepage_rule.php via the ids parameter.	9.8	More Details
CVE-2022-23336	S-CMS v5.0 was discovered to contain a SQL injection vulnerability in member_pay.php via the O_id parameter.	9.8	More Details
CVE-2022-23335	Metinfo v7.5.0 was discovered to contain a SQL injection vulnerability in language_general.class.php via doModifyParameter.	9.8	More Details
CVE-2022-22295	Metinfo v7.5.0 was discovered to contain a SQL injection vulnerability in parameter_admin.class.php via the table_para parameter.	9.8	More Details
CVE-2022-24988	In galois_2p8 before 0.1.2, PrimitivePolynomialField::new has an off-by-one buffer overflow for a vector.	9.8	More Details
CVE-2021-45420	Emerson Dixell XWEB-500 products are affected by arbitrary file write vulnerability in /cgi-bin/logo_extra_upload.cgi, /cgi-bin/cal_save.cgi, and /cgi-bin/lo_utils.cgi. An attacker will be able to write any file on the target system without any kind of authentication mechanism, and this can lead to denial of service and potentially remote code execution. Note: the product has not been supported since 2018 and should be removed or replaced	9.8	More Details
CVE-2022-23902	Tongda2000 v11.10 was discovered to contain a SQL injection vulnerability in export_data.php via the d_name parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24977	ImpressCMS before 1.4.2 allows unauthenticated remote code execution via ...../// directory traversal in origName or imageName, leading to unsafe interaction with the CKEditor processImage.php script. The payload may be placed in PHP_SESSION_UPLOAD_PROGRESS when the PHP installation supports upload_progress.	9.8	More Details
CVE-2022-0570	Heap-based Buffer Overflow in Homebrew mruby prior to 3.2.	9.8	More Details
CVE-2021-46362	A Server-Side Template Injection (SSTI) vulnerability in the Registration and Forgotten Password forms of Magnolia v6.2.3 and below allows attackers to execute arbitrary code via a crafted payload entered into the fullname parameter.	9.8	More Details
CVE-2021-46361	An issue in the Freemark Filter of Magnolia CMS v6.2.11 and below allows attackers to bypass security restrictions and execute arbitrary code via a crafted FreeMarker payload.	9.8	More Details
CVE-2021-23555	The package vm2 before 3.9.6 are vulnerable to Sandbox Bypass via direct access to host error objects generated by node internals during generation of a stacktraces, which can lead to execution of arbitrary code on the host machine.	9.8	More Details
CVE-2021-20001	It was discovered, that debian-edu-config, a set of configuration files used for the Debian Edu blend, before 2.12.16 configured insecure permissions for the user web shares (~/public_html), which could result in privilege escalation.	9.8	More Details
CVE-2020-26728	A vulnerability was discovered in Tenda AC9 v3.0 V15.03.06.42_multi and Tenda AC9 V1.0 V15.03.05.19(6318)_CN which allows for remote code execution via shell metacharacters in the guestuser field to the __fastcall function with a POST request.	9.8	More Details
CVE-2022-23390	An issue in the getType function of BBS Forum v5.3 and below allows attackers to upload arbitrary files.	9.8	More Details
CVE-2022-24206	Tongda2000 v11.10 was discovered to contain a SQL injection vulnerability in /mobile_seal/get_seal.php via the DEVICE_LIST parameter.	9.8	More Details
CVE-2021-46463	njs through 0.7.1, used in NGINX, was discovered to contain a control flow hijack caused by a Type Confusion vulnerability in njs_promise_perform_then().	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37354	Xerox Phaser 4622 v35.013.01.000 was discovered to contain a buffer overflow in the function sub_3226AC via the TIMEZONE variable. This vulnerability allows attackers to cause a Denial of Service (DoS) via crafted overflow data.	9.8	More Details
CVE-2022-24704	The rad_packet_recv function in opt/src/accel-pppd/radius/packet.c suffers from a buffer overflow vulnerability, whereby user input len is copied into a fixed buffer &attr->val.integer without any bound checks. If the client connects to the server and sends a large radius packet, a buffer overflow vulnerability will be triggered.	9.8	More Details
CVE-2022-24705	The rad_packet_recv function in radius/packet.c suffers from a memcpy buffer overflow, resulting in an overly-large recvfrom into a fixed buffer that causes a buffer overflow and overwrites arbitrary memory. If the server connects with a malicious client, crafted client requests can remotely trigger this vulnerability.	9.8	More Details
CVE-2022-25139	njs through 0.7.0, used in NGINX, was discovered to contain a heap use-after-free in njs_await_fulfilled.	9.8	More Details
CVE-2021-43049	The Database component of TIBCO Software Inc.'s TIBCO BusinessConnect Container Edition contains an easily exploitable vulnerability that allows an unauthenticated attacker with network access to obtain the usernames and passwords of users of the affected system. Affected releases are TIBCO Software Inc.'s TIBCO BusinessConnect Container Edition: versions 1.1.0 and below.	9.8	More Details
CVE-2022-22770	The Web Server component of TIBCO Software Inc.'s TIBCO AuditSafe contains an easily exploitable vulnerability that allows an unauthenticated attacker with network access to execute API methods on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO AuditSafe: versions 1.1.0 and below.	9.8	More Details
CVE-2021-33945	RICOH Printer series SP products 320DN, SP 325DNw, SP 320SN, SP 320SFN, SP 325SNw, SP 325SFNw, SP 330SN, Aficio SP 3500SF, SP 221S, SP 220SNw, SP 221SNw, SP 221SF, SP 220SFNw, SP 221SFNw v1.06 were discovered to contain a stack buffer overflow in the file /etc/wpa_supplicant.conf. This vulnerability allows attackers to cause a Denial of Service (DoS) via crafted overflow data.	9.8	More Details
CVE-2021-46262	Tenda AC Series Router AC11_V02.03.01.104_CN was discovered to contain a stack buffer overflow in the PPPoE module. This vulnerability allows attackers to cause a Denial of Service (DoS) via crafted overflow data.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45005	Artifex MuJS v1.1.3 was discovered to contain a heap buffer overflow which is caused by conflicting JumpList of nested try/finally statements.	9.8	More Details
CVE-2021-39658	ismsEx service is a vendor service in unisoc equipment。ismsEx service is an extension of sms system service，but it does not check the permissions of the caller，resulting in permission leaks。Third-party apps can use this service to arbitrarily modify and set system properties。Product: AndroidVersions: Android SoCAndroid ID: A-207479207	9.8	More Details
CVE-2021-46263	Tenda AC Series Router AC11_V02.03.01.104_CN was discovered to contain a stack buffer overflow in the wifiTime module. This vulnerability allows attackers to cause a Denial of Service (DoS) via crafted overflow data.	9.8	More Details
CVE-2021-46264	Tenda AC Series Router AC11_V02.03.01.104_CN was discovered to contain a stack buffer overflow in the onlineList module. This vulnerability allows attackers to cause a Denial of Service (DoS) via crafted overflow data.	9.8	More Details
CVE-2021-46265	Tenda AC Series Router AC11_V02.03.01.104_CN was discovered to contain a stack buffer overflow in the wanBasicCfg module. This vulnerability allows attackers to cause a Denial of Service (DoS) via crafted overflow data.	9.8	More Details
CVE-2021-46321	Tenda AC Series Router AC11_V02.03.01.104_CN was discovered to contain a stack buffer overflow in the wifiBasicCfg module. This vulnerability allows attackers to cause a Denial of Service (DoS) via crafted overflow data.	9.8	More Details
CVE-2021-46461	njs through 0.7.0, used in NGINX, was discovered to contain an out-of-bounds array access via njs_vmcode_typeof in /src/njs_vmcode.c.	9.8	More Details
CVE-2021-39675	In GKI_getbuf of gki_buffer.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-205729183	9.8	More Details
CVE-2022-24677	Admin.php in HYBBS2 through 2.3.2 allows remote code execution because it writes plugin-related configuration information to conf.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24954	Foxit PDF Reader before 11.2.1 and Foxit PDF Editor before 11.2.1 have a Stack-Based Buffer Overflow related to XFA, for the 'subform colSpan="-2"' and 'draw colSpan="1"' substrings.	9.8	More Details
CVE-2022-24310	A CWE-190: Integer Overflow or Wraparound vulnerability exists that could cause heap-based buffer overflow, leading to denial of service and potentially remote code execution when an attacker sends multiple specially crafted messages. Affected Product: Interactive Graphical SCADA System Data Server (V15.0.0.22020 and prior)	9.8	More Details
CVE-2022-24568	Novel-plus v3.6.0 was discovered to be vulnerable to Server-Side Request Forgery (SSRF) via user-supplied crafted input.	9.8	More Details
CVE-2021-45364	A Code Execution vulnerability exists in Statamic Version through 3.2.26 via SettingsController.php. NOTE: the vendor indicates that there was an error in publishing this CVE Record, and that all parties agree that the affected code was not used in any Statamic product	9.8	More Details
CVE-2021-25992	In Ifme, versions 1.0.0 to v.7.33.2 don’t properly invalidate a user’s session even after the user initiated logout. It makes it possible for an attacker to reuse the admin cookies either via local/network access or by other hypothetical attacks.	9.8	More Details
CVE-2022-24313	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could cause a stack-based buffer overflow potentially leading to remote code execution when an attacker sends a specially crafted message. Affected Product: Interactive Graphical SCADA System Data Server (V15.0.0.22020 and prior)	9.8	More Details
CVE-2022-24312	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists that could cause modification of an existing file by adding at end of file or create a new file in the context of the Data Server potentially leading to remote code execution when an attacker sends a specially crafted message. Affected Product: Interactive Graphical SCADA System Data Server (V15.0.0.22020 and prior)	9.8	More Details
CVE-2022-24311	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists that could cause modification of an existing file by inserting at beginning of file or create a new file in the context of the Data Server potentially leading to remote code execution when an attacker sends a specially crafted message. Affected Product: Interactive Graphical SCADA System Data Server (V15.0.0.22020 and prior)	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22813	A CWE-798: Use of Hard-coded Credentials vulnerability exists. If an attacker were to obtain the TLS cryptographic key and take active control of the Courier tunneling communication network, they could potentially observe and manipulate traffic associated with product configuration.	9.8	More Details
CVE-2022-24955	Foxit PDF Reader before 11.2.1 and Foxit PDF Editor before 11.2.1 have an Uncontrolled Search Path Element for DLL files.	9.8	More Details
CVE-2022-22810	A CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could allow an attacker to manipulate the admin after numerous attempts at guessing credentials. Affected Product: spaceLYnk (V2.6.2 and prior), Wiser for KNX (formerly homeLYnk) (V2.6.2 and prior), fellerLYnk (V2.6.2 and prior)	9.8	More Details
CVE-2022-22532	In SAP NetWeaver Application Server Java - versions KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, an unauthenticated attacker could submit a crafted HTTP server request which triggers improper shared memory buffer handling. This could allow the malicious payload to be executed and hence execute functions that could be impersonating the victim or even steal the victim's logon session.	9.8	More Details
CVE-2021-39997	There is a vulnerability of unstrict input parameter verification in the audio assembly.Successful exploitation of this vulnerability may cause out-of-bounds access.	9.8	More Details
CVE-2021-39994	There is an arbitrary address access vulnerability with the product line test code.Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.	9.8	More Details
CVE-2021-45331	An Authentication Bypass vulnerability exists in Gitea before 1.5.0, which could let a malicious user gain privileges. If captured, the TOTP code for the 2FA can be submitted correctly more than once.	9.8	More Details
CVE-2021-45330	An issue exsits in Gitea through 1.15.7, which could let a malicious user gain privileges due to client side cookies not being deleted and the session remains valid on the server side for reuse.	9.8	More Details
CVE-2021-39616	Summary:Product: AndroidVersions: Android SoCAndroid ID: A-204686438	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22803	A CWE-434: Unrestricted Upload of File with Dangerous Type vulnerability exists that could lead to remote code execution through a number of paths, when an attacker, writes arbitrary files to folders in context of the DC module, by sending constructed messages on the network. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21243 and prior)	9.8	More Details
CVE-2022-24961	In Portainer Agent before 2.11.1, an API server can continue running even if not associated with a Portainer instance in the past few days.	9.8	More Details
CVE-2021-34235	Tokheim Profleet DiaLOG 11.005.02 is affected by SQL Injection. The component is the Field__UserLogin parameter on the logon page.	9.8	More Details
CVE-2021-31932	Nokia BTS TRS web console FTM_W20_FP2_2019.08.16_0010 allows Authentication Bypass. A malicious unauthenticated user can get access to all the functionalities exposed via the web panel, circumventing the authentication process, by using URL encoding for the . (dot) character.	9.8	More Details
CVE-2022-24112	An attacker can abuse the batch-requests plugin to send requests to bypass the IP restriction of Admin API. A default configuration of Apache APISIX (with default API key) is vulnerable to remote code execution. When the admin key was changed or the port of Admin API was changed to a port different from the data panel, the impact is lower. But there is still a risk to bypass the IP restriction of Apache APISIX's data panel. There is a check in the batch-requests plugin which overrides the client IP with its real remote IP. But due to a bug in the code, this check can be bypassed.	9.8	More Details
CVE-2020-13675	Drupal's JSON:API and REST/File modules allow file uploads through their HTTP APIs. The modules do not correctly run all file validation, which causes an access bypass vulnerability. An attacker might be able to upload files that bypass the file validation process implemented by modules on the site.	9.8	More Details
CVE-2020-36062	Dairy Farm Shop Management System v1.0 was discovered to contain hardcoded credentials in the source code which allows attackers access to the control panel if compromised.	9.8	More Details
CVE-2021-22801	A CWE-269: Improper Privilege Management vulnerability exists that could cause an arbitrary command execution when the software is configured with specially crafted event actions. Affected Product: ConneXium Network Manager Software (All Versions)	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22802	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could result in remote code execution due to missing length check on user supplied data, when a constructed message is received on the network. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21243 and prior)	9.8	More Details
CVE-2022-0097	Inappropriate implementation in DevTools in Google Chrome prior to 97.0.4692.71 allowed an attacker who convinced a user to install a malicious extension to to potentially allow extension to escape the sandbox via a crafted HTML page.	9.6	More Details
CVE-2021-4201	Missing access control in ForgeRock Access Management 7.1.0 and earlier versions on all platforms allows remote unauthenticated attackers to hijack sessions, including potentially admin-level sessions. This issue affects: ForgeRock Access Management 7.1 versions prior to 7.1.1; 6.5 versions prior to 6.5.4; all previous versions.	9.6	More Details
CVE-2022-0290	Use after free in Site isolation in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.	9.6	More Details
CVE-2021-30317	Improper validation of program headers containing ELF metadata can lead to image verification bypass in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	9.3	More Details
CVE-2021-22823	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause deletion of arbitrary files in the context of the user running IGSS due to lack of validation of network messages. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21320 and prior)	9.1	More Details
CVE-2021-22805	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause deletion of arbitrary files in the context of the user running IGSS due to lack of validation of network messages. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21243 and prior)	9.1	More Details
CVE-2022-24976	Atheme IRC Services before 7.2.12, when used in conjunction with InspIRCd, allows authentication bypass by ending an IRC handshake at a certain point during a challenge-response login sequence.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22544	Solution Manager (Diagnostics Root Cause Analysis Tools) - version 720, allows an administrator to execute code on all connected Diagnostics Agents and browse files on their systems. An attacker could thereby control the managed systems. It is considered that this is a missing segregation of duty for the SAP Solution Manager administrator. Impacts of unauthorized execution of commands can lead to sensitive information disclosure, loss of system integrity and denial of service.	9.1	More Details
CVE-2022-0525	Out-of-bounds Read in Homebrew mruby prior to 3.2.	9.1	More Details
CVE-2021-44521	When running Apache Cassandra with the following configuration: enable_user_defined_functions: true enable_scripted_user_defined_functions: true enable_user_defined_functions_threads: false it is possible for an attacker to execute arbitrary code on the host. The attacker would need to have enough permissions to create user defined functions in the cluster to be able to exploit this. Note that this configuration is documented as unsafe, and will continue to be considered unsafe after this CVE.	9.1	More Details
CVE-2022-23806	Curve.IsOnCurve in crypto/elliptic in Go before 1.16.14 and 1.17.x before 1.17.7 can incorrectly return true in situations with a big.Int value that is not a valid field element.	9.1	More Details
CVE-2021-39635	ims_ex is a vendor system service used to manage VoLTE in unisoc devices，But it does not verify the caller's permissions，so that normal apps (No phone permissions) can obtain some VoLTE sensitive information and manage VoLTE calls.Product: AndroidVersions: Android SoCAndroid ID: A-206492634	9.1	More Details
CVE-2022-23631	superjson is a program to allow JavaScript expressions to be serialized to a superset of JSON. In versions prior to 1.8.1 superjson allows input to run arbitrary code on any server using superjson input without prior authentication or knowledge. The only requirement is that the server implements at least one endpoint which uses superjson during request processing. This has been patched in superjson 1.8.1. Users are advised to update. There are no known workarounds for this issue.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2022-24676	update_code in Admin.php in HYBBS2 through 2.3.2 allows arbitrary file upload via a crafted ZIP archive.	8.8	More Details
CVE-2021-4100	Object lifecycle issue in ANGLE in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0296	Use after free in Printing in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced the user to engage is specific user interactions to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0295	Use after free in Omnibox in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced the user to engage is specific user interactions to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-25174	Jenkins Pipeline: Shared Groovy Libraries Plugin 552.vd9cc05b8a2e1 and earlier uses the same checkout directories for distinct SCMs for Pipeline libraries, allowing attackers with Item/Configure permission to invoke arbitrary OS commands on the controller through crafted SCM contents.	8.8	More Details
CVE-2022-21984	Windows DNS Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-0293	Use after free in Web packaging in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-25175	Jenkins Pipeline: Multibranch Plugin 706.vd43c65dec013 and earlier uses the same checkout directories for distinct SCMs for the readTrusted step, allowing attackers with Item/Configure permission to invoke arbitrary OS commands on the controller through crafted SCM contents.	8.8	More Details
CVE-2021-4099	Use after free in Swiftshader in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0289	Use after free in Safe browsing in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40044	There is a permission verification vulnerability in the Bluetooth module.Successful exploitation of this vulnerability may cause unauthorized operations.	8.8	More Details
CVE-2022-22854	An access control issue in hprms/admin/?page=user/list of Hospital Patient Record Management System v1.0 allows attackers to escalate privileges via accessing and editing the user list.	8.8	More Details
CVE-2022-0115	Uninitialized use in File API in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.	8.8	More Details
CVE-2021-0163	Improper Validation of Consistency within input in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2021-0162	Improper input validation in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2021-4101	Heap buffer overflow in Swiftshader in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-4102	Use after free in V8 in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0107	Use after free in File Manager API in Google Chrome on Chrome OS prior to 97.0.4692.71 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-22808	A CWE-352: Cross-Site Request Forgery (CSRF) exists that could cause a remote attacker to gain unauthorized access to the product when conducting cross-domain attacks based on same-origin policy or cross-site request forgery protections bypass. Affected Product: EcoStruxure EV Charging Expert (formerly known as EVlink Load Management System): (HMIBSCEA53D1EDB, HMIBSCEA53D1EDS, HMIBSCEA53D1EDM, HMIBSCEA53D1EDL, HMIBSCEA53D1ESS, HMIBSCEA53D1ESM, HMIBSCEA53D1EML) (All Versions prior to SP8 (Version 01) V4.0.0.13)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-16864	CompleteFTPService.exe in the server in EnterpriseDT CompleteFTP before 12.1.4 allows Remote Code Execution by leveraging a Windows user account that has SSH access. The exec command is always run as SYSTEM.	8.8	More Details
CVE-2022-0297	Use after free in Vulkan in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-23616	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible for an unprivileged user to perform a remote code execution by injecting a groovy script in her own profile and by calling the Reset password feature since the feature is performing a save of the user profile with programming rights in the impacted versions of XWiki. The issue has been patched in XWiki 13.1RC1. There are two different possible workarounds, each consisting of modifying the XWiki/ResetPassword page. 1. The Reset password feature can be entirely disabled by deleting the XWiki/ResetPassword page. 2. The script in XWiki/ResetPassword can also be modified or removed: an administrator can replace it with a simple email contact to ask an administrator to reset the password.	8.8	More Details
CVE-2021-46366	An issue in the Login page of Magnolia CMS v6.2.3 and below allows attackers to exploit both an Open Redirect vulnerability and Cross-Site Request Forgery (CSRF) in order to brute force and exfiltrate users' credentials.	8.8	More Details
CVE-2022-0298	Use after free in Scheduling in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0311	Heap buffer overflow in Task Manager in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-23384	YzmCMS v6.3 is affected by Cross Site Request Forgery (CSRF) in /admin.add	8.8	More Details
CVE-2021-41552	CommScope SURFboard SBG6950AC2 9.1.103AA23 devices allow Command Injection.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0310	Heap buffer overflow in Task Manager in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via specific user interactions.	8.8	More Details
CVE-2021-22954	A cross-site request forgery vulnerability exists in Concrete CMS <v9 that could allow an attacker to make requests on behalf of other users.	8.8	More Details
CVE-2022-0190	The Ad Invalid Click Protector (AICP) WordPress plugin before 1.2.6 is affected by a SQL Injection in the id parameter of the delete action.	8.8	More Details
CVE-2021-44892	A Remote Code Execution (RCE) vulnerability exists in ThinkPHP 3.x.x via value[_filename] in index.php, which could let a malicious user obtain server control privileges.	8.8	More Details
CVE-2022-0308	Use after free in Data Transfer in Google Chrome on Chrome OS prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0307	Use after free in Optimization Guide in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-23604	x26-Cogs is a repository of cogs made by Twentysix for the Red Discord bot. Among these cogs is the Defender cog, a tool for Discord server moderation. A vulnerability in the Defender cog prior to version 1.10.0 allows users with admin privileges to issue commands as other users who share the same server. If a bot owner shares the same server as the attacker, it is possible for the attacker to issue bot-owner restricted commands. The issue has been patched in version 1.10.0. One may unload the Defender cog as a workaround.	8.8	More Details
CVE-2022-0306	Heap buffer overflow in PDFium in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-22005	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0304	Use after free in Bookmarks in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0302	Use after free in Omnibox in Google Chrome prior to 97.0.4692.99 allowed an attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-25173	Jenkins Pipeline: Groovy Plugin 2648.va9433432b33c and earlier uses the same checkout directories for distinct SCMs when reading the script file (typically Jenkinsfile) for Pipelines, allowing attackers with Item/Configure permission to invoke arbitrary OS commands on the controller through crafted SCM contents.	8.8	More Details
CVE-2021-33115	Improper input validation for some Intel(R) PROSet/Wireless WiFi in UEFI may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	8.8	More Details
CVE-2022-0300	Use after free in Text Input Method Editor in Google Chrome on Android prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-25181	A sandbox bypass vulnerability in Jenkins Pipeline: Shared Groovy Libraries Plugin 552.vd9cc05b8a2e1 and earlier allows attackers with Item/Configure permission to execute arbitrary code in the context of the Jenkins controller JVM through crafted SCM contents, if a global Pipeline library already exists.	8.8	More Details
CVE-2022-23274	Microsoft Dynamics GP Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-0106	Use after free in Autofill in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who convinced a user to perform specific user gesture to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-0096	Use after free in Storage in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25205	A cross-site request forgery (CSRF) vulnerability in Jenkins dbCharts Plugin 0.5.2 and earlier allows attackers to connect to an attacker-specified database via JDBC using attacker-specified credentials and to determine if a class is available in the Jenkins instance.	8.8	More Details
CVE-2022-25199	A missing permission check in Jenkins SCP publisher Plugin 1.8 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified SSH server using attacker-specified credentials.	8.8	More Details
CVE-2022-25198	A cross-site request forgery (CSRF) vulnerability in Jenkins SCP publisher Plugin 1.8 and earlier allows attackers to connect to an attacker-specified SSH server using attacker-specified credentials.	8.8	More Details
CVE-2022-0101	Heap buffer overflow in Bookmarks in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who convinced a user to perform specific user gesture to potentially exploit heap corruption via specific user gesture.	8.8	More Details
CVE-2022-25206	A missing check in Jenkins dbCharts Plugin 0.5.2 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified database via JDBC using attacker-specified credentials.	8.8	More Details
CVE-2022-25194	A cross-site request forgery (CSRF) vulnerability in Jenkins autonomiq Plugin 1.15 and earlier allows attackers to connect to an attacker-specified URL server using attacker-specified credentials.	8.8	More Details
CVE-2022-25207	A cross-site request forgery (CSRF) vulnerability in Jenkins Chef Sinatra Plugin 1.20 and earlier allows attackers to have Jenkins send an HTTP request to an attacker-controlled URL and have it parse an XML response.	8.8	More Details
CVE-2022-25208	A missing permission check in Jenkins Chef Sinatra Plugin 1.20 and earlier allows attackers with Overall/Read permission to have Jenkins send an HTTP request to an attacker-controlled URL and have it parse an XML response.	8.8	More Details
CVE-2022-0102	Type confusion in V8 in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-25209	Jenkins Chef Sinatra Plugin 1.20 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	8.8	More Details
CVE-2022-0103	Use after free in SwiftShader in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0098	Use after free in Screen Capture in Google Chrome on Chrome OS prior to 97.0.4692.71 allowed an attacker who convinced a user to perform specific user gestures to potentially exploit heap corruption via specific user gestures.	8.8	More Details
CVE-2022-25211	A missing permission check in Jenkins SWAMP Plugin 1.2.6 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified web server using attacker-specified credentials.	8.8	More Details
CVE-2022-25192	A cross-site request forgery (CSRF) vulnerability in Jenkins Snow Commander Plugin 1.10 and earlier allows attackers to connect to an attacker-specified webserver using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	8.8	More Details
CVE-2022-25212	A cross-site request forgery (CSRF) vulnerability in Jenkins SWAMP Plugin 1.2.6 and earlier allows attackers to connect to an attacker-specified web server using attacker-specified credentials.	8.8	More Details
CVE-2022-0104	Heap buffer overflow in ANGLE in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2021-22748	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could allow a remote code execution when a file is saved. Affected Product: C-Bus Toolkit (V1.15.9 and prior), C-Gate Server (V2.11.7 and prior)	8.8	More Details
CVE-2021-46360	Authenticated remote code execution (RCE) in Composr-CMS 10.0.39 and earlier allows remote attackers to execute arbitrary code via uploading a PHP shell through /adminzone/index.php?page=admin-commandr.	8.8	More Details
CVE-2022-0099	Use after free in Sign-in in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who convinced a user to perform specific user gestures to potentially exploit heap corruption via specific user gesture.	8.8	More Details
CVE-2022-0105	Use after free in PDF Accessibility in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-25183	Jenkins Pipeline: Shared Groovy Libraries Plugin 552.vd9cc05b8a2e1 and earlier uses the names of Pipeline libraries to create cache directories without any sanitization, allowing attackers with Item/Configure permission to execute arbitrary code in the context of the Jenkins controller JVM using specially crafted library names if a global Pipeline library configured to use caching already exists.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25182	A sandbox bypass vulnerability in Jenkins Pipeline: Shared Groovy Libraries Plugin 552.vd9cc05b8a2e1 and earlier allows attackers with Item/Configure permission to execute arbitrary code on the Jenkins controller JVM using specially crafted library names if a global Pipeline library is already configured.	8.8	More Details
CVE-2021-40360	A vulnerability has been identified in SIMATIC PCS 7 V8.2 (All versions), SIMATIC PCS 7 V9.0 (All versions), SIMATIC PCS 7 V9.1 (All versions < V9.1 SP1), SIMATIC WinCC V15 and earlier (All versions < V15 SP1 Update 7), SIMATIC WinCC V16 (All versions < V16 Update 5), SIMATIC WinCC V17 (All versions < V17 Update 2), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 19), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 6). The password hash of a local user account in the remote server could be granted via public API to a user on the affected system. An authenticated attacker could brute force the password hash and use it to login to the server.	8.8	More Details
CVE-2022-24289	Hessian serialization is a network protocol that supports object-based transmission. Apache Cayenne's optional Remote Object Persistence (ROP) feature is a web services-based technology that provides object persistence and query functionality to 'remote' applications. In Apache Cayenne 4.1 and earlier, running on non-current patch versions of Java, an attacker with client access to Cayenne ROP can transmit a malicious payload to any vulnerable third-party dependency on the server. This can result in arbitrary code execution.	8.8	More Details
CVE-2022-0100	Heap buffer overflow in Media streams API in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-25200	A cross-site request forgery (CSRF) vulnerability in Jenkins Checkmarx Plugin 2022.1.2 and earlier allows attackers to connect to an attacker-specified webserver using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	8.8	More Details
CVE-2022-23425	Improper input validation in Exynos baseband prior to SMR Feb-2022 Release 1 allows attackers to send arbitrary NAS signaling messages with fake base station.	8.6	More Details
CVE-2021-43050	The Auth Server component of TIBCO Software Inc.'s TIBCO BusinessConnect Container Edition contains an easily exploitable vulnerability that allows an unauthenticated attacker with local access to obtain administrative usernames and passwords for the affected system. Affected releases are TIBCO Software Inc.'s TIBCO BusinessConnect Container Edition: versions 1.1.0 and below.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35075	Possible null pointer dereference due to lack of WDOG structure validation during registration in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2021-35077	Possible use after free scenario in compute offloads to DSP while multiple calls spawn a dynamic process in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2021-35074	Possible integer overflow due to improper fragment datatype while calculating number of fragments in a request message in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details
CVE-2022-0162	The vulnerability exists in TP-Link TL-WR841N V11 3.16.9 Build 160325 Rel.62500n wireless router due to transmission of authentication information in cleartextbase64 format. Successful exploitation of this vulnerability could allow a remote attacker to intercept credentials and subsequently perform administrative operations on the affected device through web-based management interface.	8.4	More Details
CVE-2022-23428	An improper boundary check in eden_runtime hal service prior to SMR Feb-2022 Release 1 allows arbitrary memory write and code execution.	8.4	More Details
CVE-2022-0185	A heap-based buffer overflow flaw was found in the way the legacy_parse_param function in the Filesystem Context functionality of the Linux kernel verified the supplied parameters length. An unprivileged (in case of unprivileged user namespaces enabled, otherwise needs namespaced CAP_SYS_ADMIN privilege) local user able to open a filesystem that does not support the Filesystem Context API (and thus fallbacks to legacy handling) could use this flaw to escalate their privileges on the system.	8.4	More Details
CVE-2021-35068	Lack of null check while freeing the device information buffer in the Bluetooth HFP protocol can lead to a NULL pointer dereference in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2021-0066	Improper input validation in firmware for Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable escalation of privilege via local access.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30318	Improper validation of input when provisioning the HDCP key can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables	8.4	More Details
CVE-2020-14521	Multiple Mitsubishi Electric Factory Automation engineering software products have a malicious code execution vulnerability. A malicious attacker could use this vulnerability to obtain information, modify information, and cause a denial-of-service condition.	8.3	More Details
CVE-2020-14523	Multiple Mitsubishi Electric Factory Automation products have a vulnerability that allows an attacker to execute arbitrary code.	8.3	More Details
CVE-2022-0114	Out of bounds memory access in Blink Serial API in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page and virtual serial port driver.	8.1	More Details
CVE-2022-23272	Microsoft Dynamics GP Elevation Of Privilege Vulnerability	8.1	More Details
CVE-2022-23256	Azure Data Explorer Spoofing Vulnerability	8.1	More Details
CVE-2022-23639	crossbeam-utils provides atomics, synchronization primitives, scoped threads, and other utilities for concurrent programming in Rust. crossbeam-utils prior to version 0.8.7 incorrectly assumed that the alignment of `{i,u}64` was always the same as `Atomic{I,U}64`. However, the alignment of `{i,u}64` on a 32-bit target can be smaller than `Atomic{I,U}64`. This can cause unaligned memory accesses and data race. Crates using `fetch_*` methods with `AtomicCell<{i,u}64>` are affected by this issue. 32-bit targets without `Atomic{I,U}64` and 64-bit targets are not affected by this issue. This has been fixed in crossbeam-utils 0.8.7. There are currently no known workarounds.	8.1	More Details
CVE-2021-26613	improper input validation vulnerability in nexacro permits copying file to the startup folder using rename method.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22811	A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists that could induce users to perform unintended actions, leading to the override of the system's configurations when an attacker persuades a user to visit a rogue website. Affected Product: spaceLYnk (V2.6.2 and prior), Wiser for KNX (formerly homeLYnk) (V2.6.2 and prior), fellerLYnk (V2.6.2 and prior)	8.1	More Details
CVE-2022-21991	Visual Studio Code Remote Development Extension Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-21660	Gin-vue-admin is a backstage management system based on vue and gin. In versions prior to 2.4.7 low privilege users are able to modify higher privilege users. Authentication is missing on the `setUserInfo` function. Users are advised to update as soon as possible. There are no known workarounds.	8.1	More Details
CVE-2022-24647	Cuppa CMS v1.0 was discovered to contain an arbitrary file deletion vulnerability via the unlink() function.	8.1	More Details
CVE-2021-33113	Improper input validation for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and Killer(TM) WiFi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service or information disclosure via adjacent access.	8.1	More Details
CVE-2022-21987	Microsoft SharePoint Server Spoofing Vulnerability	8.0	More Details
CVE-2022-22765	BD Viper LT system, versions 2.0 and later, contains hardcoded credentials. If exploited, threat actors may be able to access, modify or delete sensitive information, including electronic protected health information (ePHI), protected health information (PHI) and personally identifiable information (PII). BD Viper LT system versions 4.0 and later utilize Microsoft Windows 10 and have additional Operating System hardening configurations which increase the attack complexity required to exploit this vulnerability.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23634	Puma is a Ruby/Rack web server built for parallelism. Prior to `puma` version `5.6.2`, `puma` may not always call `close` on the response body. Rails, prior to version `7.0.2.2`, depended on the response body being closed in order for its `CurrentAttributes` implementation to work correctly. The combination of these two behaviors (Puma not closing the body + Rails' Executor implementation) causes information leakage. This problem is fixed in Puma versions 5.6.2 and 4.3.11. This problem is fixed in Rails versions 7.02.2, 6.1.4.6, 6.0.4.6, and 5.2.6.2. Upgrading to a patched Rails _or_ Puma version fixes the vulnerability.	8.0	More Details
CVE-2022-21995	Windows Hyper-V Remote Code Execution Vulnerability	7.9	More Details
CVE-2021-0156	Improper input validation in the firmware for some Intel(R) Processors may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2022-0572	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2021-45444	In zsh before 5.8.1, an attacker can achieve code execution if they control a command output inside the prompt, as demonstrated by a %F argument. This occurs because of recursive PROMPT_SUBST expansion.	7.8	More Details
CVE-2021-0164	Improper access control in firmware for Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-46363	An issue in the Export function of Magnolia v6.2.3 and below allows attackers to perform Formula Injection attacks via crafted CSV/XLS files. These formulas may result in arbitrary code execution on a victim's computer when opening the exported files with Microsoft Excel.	7.8	More Details
CVE-2022-0483	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis VSS Doctor (Windows) before build 53	7.8	More Details
CVE-2021-46364	A vulnerability in the Snake YAML parser of Magnolia CMS v6.2.3 and below allows attackers to execute arbitrary code via a crafted YAML file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46365	An issue in the Export function of Magnolia v6.2.3 and below allows attackers to execute XML External Entity attacks via a crafted XLF file.	7.8	More Details
CVE-2022-23853	The LSP (Language Server Protocol) plugin in KDE Kate before 21.12.2 and KTextEditor before 5.91.0 tries to execute the associated LSP server binary when opening a file of a given type. If this binary is absent from the PATH, it will try running the LSP server binary in the directory of the file that was just opened (due to a misunderstanding of the QProcess API, that was never intended). This can be an untrusted directory.	7.8	More Details
CVE-2021-37109	There is a security protection bypass vulnerability with the modem.Successful exploitation of this vulnerability may cause memory protection failure.	7.8	More Details
CVE-2021-22817	A CWE-276: Incorrect Default Permissions vulnerability exists that could cause unauthorized access to the base installation directory leading to local privilege escalation. Affected Product: Harmony/Magelis iPC Series (All Versions), Vijeo Designer (All Versions prior to V6.2 SP11 Multiple HotFix 4), Vijeo Designer Basic (All Versions prior to V1.2.1)	7.8	More Details
CVE-2021-23152	Improper access control in the Intel(R) Advisor software before version 2021.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-20041	In Bluetooth, there is a possible escalation of privilege 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. Patch ID: ALPS06108596; Issue ID: ALPS06108596.	7.8	More Details
CVE-2022-20040	In power_hal_manager_service, there is a possible permission bypass due to a stack-based buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06219150; Issue ID: ALPS06219150.	7.8	More Details
CVE-2022-20045	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126820; Issue ID: ALPS06126820.	7.8	More Details
CVE-2022-20031	In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20028	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198663; Issue ID: ALPS06198663.	7.8	More Details
CVE-2022-20027	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126826; Issue ID: ALPS06126826.	7.8	More Details
CVE-2022-20026	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126827; Issue ID: ALPS06126827.	7.8	More Details
CVE-2022-20025	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126832; Issue ID: ALPS06126832.	7.8	More Details
CVE-2022-20024	In system service, there is a possible permission bypass 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. Patch ID: ALPS06219064; Issue ID: ALPS06219064.	7.8	More Details
CVE-2022-21174	Improper access control in a third-party component of Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-21203	Improper permissions in the SafeNet Sentinel driver for Intel(R) Quartus(R) Prime Standard Edition before version 21.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-21204	Improper permissions for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-44454	Improper input validation in a third-party component for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-39992	There is an improper security permission configuration vulnerability on ACPU.Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21220	Improper restriction of XML external entity for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-0116	Out-of-bounds write in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2022-21825	An Improper Access Control vulnerability exists in Citrix Workspace App for Linux 2012 - 2111 with App Protection installed that can allow an attacker to perform local privilege escalation.	7.8	More Details
CVE-2021-33137	Out-of-bounds write in the Intel(R) Kernelflinger project may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-33129	Incorrect default permissions in the software installer for the Intel(R) Advisor before version 2021.4.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2022-0301	Heap buffer overflow in DevTools in Google Chrome prior to 97.0.4692.99 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	7.8	More Details
CVE-2022-22528	SAP Adaptive Server Enterprise (ASE) - version 16.0, installation makes an entry in the system PATH environment variable in Windows platform which, under certain conditions, allows a Standard User to execute malicious Windows binaries which may lead to privilege escalation on the local system. The issue is with the ASE installer and does not impact other ASE binaries.	7.8	More Details
CVE-2021-33101	Uncontrolled search path in the Intel(R) GPA software before version 21.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2021-26616	An OS command injection was found in SecuwaySSL, when special characters injection on execute command with runCommand arguments.	7.8	More Details
CVE-2021-0117	Pointer issues in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39669	In onCreate of InstallCaCertificateWarning.java, there is a possible way to mislead an user about CA installation circumstances due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-196969991	7.8	More Details
CVE-2022-21994	Windows DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21974	Roaming Security Rights Management Services Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-46159	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15050)	7.8	More Details
CVE-2021-46160	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15286)	7.8	More Details
CVE-2021-46161	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15302)	7.8	More Details
CVE-2022-21844	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21926	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21927	HEVC Video Extensions Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21971	Windows Runtime Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21981	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-46157	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a memory corruption vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14757)	7.8	More Details
CVE-2022-0554	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2022-21988	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21989	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21992	Windows Mobile Device Management Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-21996	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-21999	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-22000	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2021-46158	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a stack based buffer overflow vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15085, ZDI-CAN-15289, ZDI-CAN-15602)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46156	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14684)	7.8	More Details
CVE-2021-22796	A CWE-287: Improper Authentication vulnerability exists that could allow remote code execution when a malicious file is uploaded. Affected Product: C-Bus Toolkit (V1.15.9 and prior), C-Gate Server (V2.11.7 and prior)	7.8	More Details
CVE-2022-24958	drivers/usb/gadget/legacy/inode.c in the Linux kernel through 5.16.8 mishandles dev->buf release.	7.8	More Details
CVE-2021-37852	ESET products for Windows allows untrusted process to impersonate the client of a pipe, which can be leveraged by attacker to escalate privileges in the context of NT AUTHORITY\SYSTEM.	7.8	More Details
CVE-2021-42714	Splashtop Remote Client (Business Edition) through 3.4.8.3 creates a Temporary File in a Directory with Insecure Permissions.	7.8	More Details
CVE-2021-42713	Splashtop Remote Client (Personal Edition) through 3.4.6.1 creates a Temporary File in a Directory with Insecure Permissions.	7.8	More Details
CVE-2021-35069	Improper validation of data length received from DMA buffer can lead to memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking	7.8	More Details
CVE-2021-30323	Improper validation of maximum size of data write to EFS file can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.8	More Details
CVE-2021-30322	Possible out of bounds write due to improper validation of number of GPIOs configured in an internal parameters array in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.8	More Details
CVE-2021-30309	Improper size validation of QXDM commands can lead to memory corruption in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40363	A vulnerability has been identified in SIMATIC PCS 7 V8.2 (All versions), SIMATIC PCS 7 V9.0 (All versions), SIMATIC PCS 7 V9.1 (All versions < V9.1 SP1), SIMATIC WinCC V15 and earlier (All versions < V15 SP1 Update 7), SIMATIC WinCC V16 (All versions < V16 Update 5), SIMATIC WinCC V17 (All versions < V17 Update 2), SIMATIC WinCC V17 (All versions <= V17 Update 4), SIMATIC WinCC V7.4 (All versions < V7.4 SP1 Update 19), SIMATIC WinCC V7.5 (All versions < V7.5 SP2 Update 6). The affected component stores the credentials of a local system account in a potentially publicly accessible project file using an outdated cipher algorithm. An attacker may use this to brute force the credentials and take over the system.	7.8	More Details
CVE-2021-46155	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a stack based buffer overflow vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14683, ZDI-CAN-15283, ZDI-CAN-15303, ZDI-CAN-15593)	7.8	More Details
CVE-2021-44000	A vulnerability has been identified in JT2Go (All versions < V13.2.0.7), Solid Edge SE2021 (All versions < SE2021MP9), Solid Edge SE2022 (All versions < SE2022MP1), Teamcenter Visualization V13.1 (All versions < V13.1.0.9), Teamcenter Visualization V13.2 (All versions < V13.2.0.7), Teamcenter Visualization V13.3 (All versions < V13.3.0.1). The plmxmlAdapterSE70.dll contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15053)	7.8	More Details
CVE-2021-44016	A vulnerability has been identified in JT2Go (All versions < V13.2.0.7), Solid Edge SE2021 (All versions < SE2021MP9), Solid Edge SE2022 (All versions < SE2022MP1), Teamcenter Visualization V13.1 (All versions < V13.1.0.9), Teamcenter Visualization V13.2 (All versions < V13.2.0.7), Teamcenter Visualization V13.3 (All versions < V13.3.0.1). The plmxmlAdapterSE70.dll library is vulnerable to memory corruption condition while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15110)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44018	A vulnerability has been identified in JT2Go (All versions < V13.2.0.7), Solid Edge SE2021 (All versions < SE2021MP9), Solid Edge SE2022 (All versions < SE2022MP1), Teamcenter Visualization V13.1 (All versions < V13.1.0.9), Teamcenter Visualization V13.2 (All versions < V13.2.0.7), Teamcenter Visualization V13.3 (All versions < V13.3.0.1). The plmxmlAdapterSE70.dll library is vulnerable to memory corruption condition while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-15112)	7.8	More Details
CVE-2021-46151	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14754, ZDI-CAN-15082)	7.8	More Details
CVE-2021-46152	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a type confusion vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14643, ZDI-CAN-14644, ZDI-CAN-14755, ZDI-CAN-15183)	7.8	More Details
CVE-2021-46153	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a memory corruption vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14645, ZDI-CAN-15305, ZDI-CAN-15589, ZDI-CAN-15599)	7.8	More Details
CVE-2021-46154	A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a stack based buffer overflow vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14646, ZDI-CAN-14679, ZDI-CAN-15084, ZDI-CAN-15304)	7.8	More Details
CVE-2022-22001	Windows Remote Access Connection Manager Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-20043	In Bluetooth, there is a possible escalation of privilege 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. Patch ID: ALPS06148177; Issue ID: ALPS06148177.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22003	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-39619	In updatePackageMappingsData of UsageStatsService.java, there is a possible way to bypass security and privacy settings of app usage due to an unusual root cause. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-197399948	7.8	More Details
CVE-2021-0099	Insufficient control flow management in the firmware for some Intel(R) Processors may allow an authenticated user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2022-25150	In Malwarebytes Binisoft Windows Firewall Control before 6.8.1.0, programs executed from the Tools tab can be used to escalate privileges.	7.8	More Details
CVE-2021-0091	Improper access control in the firmware for some Intel(R) Processors may allow an unauthenticated user to potentially enable an escalation of privilege via local access.	7.8	More Details
CVE-2021-39676	In writeThrowable of AndroidFuture.java, there is a possible parcel serialization/deserialization mismatch 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.Product: AndroidVersions: Android-11Android ID: A-197228210	7.8	More Details
CVE-2022-23410	AXIS IP Utility before 4.18.0 allows for remote code execution and local privilege escalation by the means of DLL hijacking. IPUtility.exe would attempt to load DLLs from its current working directory which could allow for remote code execution if a compromised DLL would be placed in the same folder.	7.8	More Details
CVE-2021-39674	In btm_sec_connected and btm_sec_disconnected of btm_sec.cc file , there is a possible use after free. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-201083442	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43940	Affected versions of Atlassian Confluence Server and Data Center allow authenticated local attackers to achieve elevated privileges on the local system via a DLL Hijacking vulnerability in the Confluence installer. This vulnerability only affects installations of Confluence Server and Data Center on Windows. The affected versions are before version 7.4.10, and from version 7.5.0 before 7.12.3.	7.8	More Details
CVE-2021-39672	In fastboot, there is a possible secure boot bypass due to a configuration error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android SoC Android ID: A-202018701	7.8	More Details
CVE-2022-22004	Microsoft Office ClickToRun Remote Code Execution Vulnerability	7.8	More Details
CVE-2021-39668	In onActivityViewReady of DetailDialog.kt, there is a possible Intent Redirect due to a confused deputy. This could lead to local escalation of privilege that allows actions performed as the System UI, with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-193445603	7.8	More Details
CVE-2021-39663	In openFileAndEnforcePathPermissionsHelper of MediaProvider.java, there is a possible bypass of a permissions check due to a confused deputy. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-200682135	7.8	More Details
CVE-2021-39662	In checkUriPermission of MediaProvider.java , there is a possible way to gain access to the content of media provider collections due to a missing permission check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-197302116	7.8	More Details
CVE-2022-23276	SQL Server for Linux Containers Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-20044	In Bluetooth, there is a possible service crash due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126814; Issue ID: ALPS06126814.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42712	Splashtop Streamer through 3.4.8.3 creates a Temporary File in a Directory with Insecure Permissions.	7.8	More Details
CVE-2022-22709	VP9 Video Extensions Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-22715	Named Pipe File System Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-22718	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-0565	Cross-site Scripting in Packagist pimcore/pimcore prior to 10.3.1.	7.6	More Details
CVE-2021-22798	A CWE-522: Insufficiently Protected Credentials vulnerability exists that could cause Sensitive data such as login credentials being exposed when a Network is sniffed. Affected Product: Conext&#65533; ComBox (All Versions)	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24667	A program using swift-nio-http2 is vulnerable to a denial of service attack, caused by a network peer sending a specially crafted HPACK-encoded header block. This attack affects all swift-nio-http2 versions from 1.0.0 to 1.19.1. There are a number of implementation errors in the parsing of HPACK-encoded header blocks that allow maliciously crafted HPACK header blocks to cause crashes in processes using swift-nio-http2. Each of these crashes is triggered instead of an integer overflow. A malicious HPACK header block could be sent on any of the HPACK-carrying frames in a HTTP/2 connection (HEADERS and PUSH_PROMISE), at any position. Sending a HPACK header block does not require any special permission, so any HTTP/2 connection peer may send one. For clients, this means any server to which they connect may launch this attack. For servers, anyone they allow to connect to them may launch such an attack. The attack is low-effort: it takes very little resources to send an appropriately crafted field block. The impact on availability is high: receiving a frame carrying this field block immediately crashes the server, dropping all in-flight connections and causing the service to need to restart. It is straightforward for an attacker to repeatedly send appropriately crafted field blocks, so attackers require very few resources to achieve a substantial denial of service. The attack does not have any confidentiality or integrity risks in and of itself: swift-nio-http2 is parsing the field block in memory-safe code and the crash is triggered instead of an integer overflow. However, sudden process crashes can lead to violations of invariants in services, so it is possible that this attack can be used to trigger an error condition that has confidentiality or integrity risks. The risk can be mitigated if untrusted peers can be prevented from communicating with the service. This mitigation is not available to many services. The issue is fixed by rewriting the parsing code to correctly handle all conditions in the function. The principal issue was found by automated fuzzing by oss-fuzz, but several associated bugs in the same code were found by code audit and fixed at the same time	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24666	A program using swift-nio-http2 is vulnerable to a denial of service attack, caused by a network peer sending a specially crafted HTTP/2 frame. This attack affects all swift-nio-http2 versions from 1.0.0 to 1.19.1. This vulnerability is caused by a logical error when parsing a HTTP/2 HEADERS frame where the frame contains priority information without any other data. This logical error caused confusion about the size of the frame, leading to a parsing error. This parsing error immediately crashes the entire process. Sending a HEADERS frame with HTTP/2 priority information does not require any special permission, so any HTTP/2 connection peer may send such a frame. For clients, this means any server to which they connect may launch this attack. For servers, anyone they allow to connect to them may launch such an attack. The attack is low-effort: it takes very little resources to send an appropriately crafted frame. The impact on availability is high: receiving the frame immediately crashes the server, dropping all in-flight connections and causing the service to need to restart. It is straightforward for an attacker to repeatedly send appropriately crafted frames, so attackers require very few resources to achieve a substantial denial of service. The attack does not have any confidentiality or integrity risks in and of itself: swift-nio-http2 is parsing the frame in memory-safe code, so the crash is safe. However, sudden process crashes can lead to violations of invariants in services, so it is possible that this attack can be used to trigger an error condition that has confidentiality or integrity risks. The risk can be mitigated if untrusted peers can be prevented from communicating with the service. This mitigation is not available to many services. The issue is fixed by rewriting the parsing code to correctly handle the condition. The issue was found by automated fuzzing by oss-fuzz.	7.5	More Details
CVE-2022-24321	A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists that could cause Denial of Service against the Geo SCADA server when receiving a malformed HTTP request. Affected Product: ClearSCADA (All Versions), EcoStruxure Geo SCADA Expert 2019 (All Versions), EcoStruxure Geo SCADA Expert 2020 (All Versions)	7.5	More Details
CVE-2021-39677	In startVideoStream() there is a possibility of an OOB Read in the heap, when the camera buffer is ‘zero’ in size.Product: AndroidVersions: Android-11Android ID: A-205097028	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23630	Gradle is a build tool with a focus on build automation and support for multi-language development. In some cases, Gradle may skip that verification and accept a dependency that would otherwise fail the build as an untrusted external artifact. This occurs when dependency verification is disabled on one or more configurations and those configurations have common dependencies with other configurations that have dependency verification enabled. If the configuration that has dependency verification disabled is resolved first, Gradle does not verify the common dependencies for the configuration that has dependency verification enabled. Gradle 7.4 fixes that issue by validating artifacts at least once if they are present in a resolved configuration that has dependency verification active. For users who cannot update either do not use `ResolutionStrategy.disableDependencyVerification()` and do not use plugins that use that method to disable dependency verification for a single configuration or make sure resolution of configuration that disable that feature do not happen in builds that resolve configuration where the feature is enabled.	7.5	More Details
CVE-2021-22787	A CWE-20: Improper Input Validation vulnerability exists that could cause denial of service of the device when an attacker sends a specially crafted HTTP request to the web server of the device. Affected Product: Modicon M340 CPUs: BMXP34 (Versions prior to V3.40), Modicon M340 X80 Ethernet Communication Modules: BMXNOE0100 (H), BMXNOE0110 (H), BMXNOC0401, BMXNOR0200H RTU (All Versions), Modicon Premium Processors with integrated Ethernet (Copro): TSXP574634, TSXP575634, TSXP576634 (All Versions), Modicon Quantum Processors with Integrated Ethernet (Copro): 140CPU65xxxxx (All Versions), Modicon Quantum Communication Modules: 140NOE771x1, 140NOC78x00, 140NOC77101 (All Versions), Modicon Premium Communication Modules: TSXETY4103, TSXETY5103 (All Versions)	7.5	More Details
CVE-2021-30326	Possible assertion due to improper size validation while processing the DownlinkPreemption IE in an RRC Reconfiguration/RRC Setup message in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	7.5	More Details
CVE-2022-24318	A CWE-326: Inadequate Encryption Strength vulnerability exists that could cause non-encrypted communication with the server when outdated versions of the ViewX client are used. Affected Product: ClearSCADA (All Versions), EcoStruxure Geo SCADA Expert 2019 (All Versions), EcoStruxure Geo SCADA Expert 2020 (All Versions)	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24317	A CWE-862: Missing Authorization vulnerability exists that could cause information exposure when an attacker sends a specific message. Affected Product: Interactive Graphical SCADA System Data Server (V15.0.0.22020 and prior)	7.5	More Details
CVE-2022-24314	A CWE-125: Out-of-bounds Read vulnerability exists that could cause memory leaks potentially resulting in denial of service when an attacker repeatedly sends a specially crafted message. Affected Product: Interactive Graphical SCADA System Data Server (V15.0.0.22020 and prior)	7.5	More Details
CVE-2021-23597	This affects the package fastify-multipart before 5.3.1. By providing a name=constructor property it is still possible to crash the application. **Note:** This is a bypass of CVE-2020-8136 (https://security.snyk.io/vuln/SNYK-JS-FASTIFYMULTIPART-1290382).	7.5	More Details
CVE-2020-13677	Under some circumstances, the Drupal core JSON:API module does not properly restrict access to certain content, which may result in unintended access bypass. Sites that do not have the JSON:API module enabled are not affected.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24668	A program using swift-nio-http2 is vulnerable to a denial of service attack caused by a network peer sending ALTSVC or ORIGIN frames. This attack affects all swift-nio-http2 versions from 1.0.0 to 1.19.1. This vulnerability is caused by a logical error after frame parsing but before frame handling. ORIGIN and ALTSVC frames are not currently supported by swift-nio-http2, and should be ignored. However, one code path that encounters them has a deliberate trap instead. This was left behind from the original development process and was never removed. Sending an ALTSVC or ORIGIN frame does not require any special permission, so any HTTP/2 connection peer may send such a frame. For clients, this means any server to which they connect may launch this attack. For servers, anyone they allow to connect to them may launch such an attack. The attack is low-effort: it takes very little resources to send one of these frames. The impact on availability is high: receiving the frame immediately crashes the server, dropping all in-flight connections and causing the service to need to restart. It is straightforward for an attacker to repeatedly send these frames, so attackers require very few resources to achieve a substantial denial of service. The attack does not have any confidentiality or integrity risks in and of itself. This is a controlled, intentional crash. However, sudden process crashes can lead to violations of invariants in services, so it is possible that this attack can be used to trigger an error condition that has confidentiality or integrity risks. The risk can be mitigated if untrusted peers can be prevented from communicating with the service. This mitigation is not available to many services. The issue is fixed by rewriting the parsing code to correctly handle the condition. The issue was found by automated fuzzing by oss-fuzz.	7.5	More Details
CVE-2022-23772	Rat.SetString in math/big in Go before 1.16.14 and 1.17.x before 1.17.7 has an overflow that can lead to Uncontrolled Memory Consumption.	7.5	More Details
CVE-2022-23773	cmd/go in Go before 1.16.14 and 1.17.x before 1.17.7 can misinterpret branch names that falsely appear to be version tags. This can lead to incorrect access control if an actor is supposed to be able to create branches but not tags.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22788	A CWE-787: Out-of-bounds Write vulnerability exists that could cause denial of service when an attacker sends a specially crafted HTTP request to the web server of the device. Affected Product: Modicon M340 CPUs: BMXP34 (Versions prior to V3.40), Modicon M340 X80 Ethernet Communication Modules: BMXNOE0100 (H), BMXNOE0110 (H), BMXNOC0401, BMXNOR0200H RTU (All Versions), Modicon Premium Processors with integrated Ethernet (Copro): TSXP574634, TSXP575634, TSXP576634 (All Versions), Modicon Quantum Processors with Integrated Ethernet (Copro): 140CPU65xxxxx (All Versions), Modicon Quantum Communication Modules: 140NOE771x1, 140NOC78x00, 140NOC77101 (All Versions), Modicon Premium Communication Modules: TSXETY4103, TSXETY5103 (All Versions)	7.5	More Details
CVE-2022-24975	The --mirror documentation for Git through 2.35.1 does not mention the availability of deleted content, aka the "GitBleed" issue. This could present a security risk if information-disclosure auditing processes rely on a clone operation without the --mirror option. Note: This has been disputed by multiple 3rd parties who believe this is an intended feature of the git binary and does not pose a security risk.	7.5	More Details
CVE-2022-24316	A CWE-665: Improper Initialization vulnerability exists that could cause information exposure when an attacker sends a specially crafted message. Affected Product: Interactive Graphical SCADA System Data Server (V15.0.0.22020 and prior)	7.5	More Details
CVE-2022-22543	SAP NetWeaver Application Server for ABAP (Kernel) and ABAP Platform (Kernel) - versions KERNEL 7.22, 8.04, 7.49, 7.53, 7.77, 7.81, 7.85, 7.86, 7.87, KRNL64UC 8.04, 7.22, 7.22EXT, 7.49, 7.53, KRNL64NUC 7.22, 7.22EXT, 7.49, does not sufficiently validate sap-passport information, which could lead to a Denial-of-Service attack. This allows an unauthorized remote user to provoke a breakdown of the SAP Web Dispatcher or Kernel work process. The crashed process can be restarted immediately, other processes are not affected.	7.5	More Details
CVE-2022-24916	Optimism before @eth-optimism/l2geth@0.5.11 allows economic griefing because a balance is duplicated upon contract self-destruction.	7.5	More Details
CVE-2022-22540	SAP NetWeaver AS ABAP (Workplace Server) - versions 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 787, allows an attacker to execute crafted database queries, that could expose the backend database. Successful attacks could result in disclosure of a table of contents from the system, but no risk of modification possible.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22800	A CWE-20: Improper Input Validation vulnerability exists that could cause a Denial of Service when a crafted packet is sent to the controller over network port 1105/TCP. Affected Product: Modicon M218 Logic Controller (V5.1.0.6 and prior)	7.5	More Details
CVE-2021-22804	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists that could cause disclosure of arbitrary files being read in the context of the user running IGSS, due to missing validation of user supplied data in network messages. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21243 and prior)	7.5	More Details
CVE-2021-22806	A CWE-669: Incorrect Resource Transfer Between Spheres vulnerability exists that could cause data exfiltration and unauthorized access when accessing a malicious website. Affected Product: spaceLYnk (V2.6.1 and prior), Wiser for KNX (V2.6.1 and prior), fellerLYnk (V2.6.1 and prior)	7.5	More Details
CVE-2021-22824	A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could result in denial of service, due to missing length check on user-supplied data from a constructed message received on the network. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21320 and prior)	7.5	More Details
CVE-2022-24646	Hospital Management System v4.0 was discovered to contain a SQL injection vulnerability in /Hospital-Management-System-master/contact.php via the txtMsg parameters.	7.5	More Details
CVE-2021-22785	A CWE-200: Information Exposure vulnerability exists that could cause sensitive information of files located in the web root directory to leak when an attacker sends a HTTP request to the web server of the device. Affected Product: Modicon M340 CPUs: BMXP34 (Versions prior to V3.40), Modicon M340 X80 Ethernet Communication Modules: BMXNOE0100 (H), BMXNOE0110 (H), BMXNOC0401, BMXNOR0200H RTU (All Versions), Modicon Premium Processors with integrated Ethernet (Copro): TSXP574634, TSXP575634, TSXP576634 (All Versions), Modicon Quantum Processors with Integrated Ethernet (Copro): 140CPU65xxxxx (All Versions), Modicon Quantum Communication Modules: 140NOE771x1, 140NOC78x00, 140NOC77101 (All Versions), Modicon Premium Communication Modules: TSXETY4103, TSXETY5103 (All Versions)	7.5	More Details
CVE-2022-21205	Improper restriction of XML external entity reference in DSP Builder Pro for Intel(R) Quartus(R) Prime Pro Edition before version 21.3 may allow an unauthenticated user to potentially enable information disclosure via network access.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22533	Due to improper error handling in SAP NetWeaver Application Server Java - versions KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, an attacker could submit multiple HTTP server requests resulting in errors, such that it consumes the memory buffer. This could result in system shutdown rendering the system unavailable.	7.5	More Details
CVE-2022-24315	A CWE-125: Out-of-bounds Read vulnerability exists that could cause denial of service when an attacker repeatedly sends a specially crafted message. Affected Product: Interactive Graphical SCADA System Data Server (V15.0.0.22020 and prior)	7.5	More Details
CVE-2020-13670	Information Disclosure vulnerability in file module of Drupal Core allows an attacker to gain access to the file metadata of a permanent private file that they do not have access to by guessing the ID of the file. This issue affects: Drupal Core 8.8.x versions prior to 8.8.10; 8.9.x versions prior to 8.9.6; 9.0.x versions prior to 9.0.6.	7.5	More Details
CVE-2021-43734	kkFileview v4.0.0 has arbitrary file read through a directory traversal vulnerability which may lead to sensitive file leak on related host.	7.5	More Details
CVE-2022-24226	Hospital Management System v4.0 was discovered to contain a blind SQL injection vulnerability via the register function in func2.php.	7.5	More Details
CVE-2022-23317	CobaltStrike <=4.5 HTTP(S) listener does not determine whether the request URL begins with "/", and attackers can obtain relevant information by specifying the URL.	7.5	More Details
CVE-2021-37185	A vulnerability has been identified in SIMATIC Drive Controller family (All versions >= V2.9.2 < V2.9.4), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions >= V21.9 < V21.9.4), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions >= V4.5.0 < V4.5.2), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions >= V2.9.2 < V2.9.4), SIMATIC S7-1500 Software Controller (All versions >= V21.9 < V21.9.4), SIMATIC S7-PLCSIM Advanced (All versions >= V4.0 < V4.0 SP1), SIPLUS TIM 1531 IRC (All versions < V2.3.6), TIM 1531 IRC (All versions < V2.3.6). An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially prepared packets over port 102/tcp. A restart of the affected device is needed to restore normal operations.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45392	A Buffer Overflow vulnerability exists in Tenda Router AX12 V22.03.01.21_CN in the sub_422CE4 function in page /goform/setIPv6Status via the prefixDelegate parameter, which causes a Denial of Service.	7.5	More Details
CVE-2021-41442	An HTTP smuggling attack in the web application of D-Link DIR-X1860 before v1.10WWB09_Beta allows a remote unauthenticated attacker to DoS the web application via sending a specific HTTP packet.	7.5	More Details
CVE-2021-46371	antd-admin 5.5.0 is affected by an incorrect access control vulnerability. Unauthorized access to some interfaces in the foreground leads to leakage of sensitive information.	7.5	More Details
CVE-2021-37204	A vulnerability has been identified in SIMATIC Drive Controller family (All versions < V2.9.2), SIMATIC Drive Controller family (All versions >= V2.9.2 < V2.9.4), SIMATIC ET 200SP Open Controller CPU 1515SP PC (incl. SIPLUS variants) (All versions), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions < V21.9), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions >= V21.9 < V21.9.4), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 Ready4Linux (All versions), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions < V4.5.0), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions >= V4.5.0 < V4.5.2), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions < V2.9.2), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions >= V2.9.2 < V2.9.4), SIMATIC S7-1500 Software Controller (All versions < V21.9), SIMATIC S7-1500 Software Controller (All versions >= V21.9 < V21.9.4), SIMATIC S7-PLCSIM Advanced (All versions < V4.0), SIMATIC S7-PLCSIM Advanced (All versions >= V4.0 < V4.0 SP1), SIPLUS TIM 1531 IRC (All versions < V2.3.6), TIM 1531 IRC (All versions < V2.3.6). An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially prepared packet over port 102/tcp. A restart of the affected device is needed to restore normal operations.	7.5	More Details
CVE-2021-37194	A vulnerability has been identified in COMOS V10.2 (All versions only if web components are used), COMOS V10.3 (All versions < V10.3.3.3 only if web components are used), COMOS V10.4 (All versions < V10.4.1 only if web components are used). The COMOS Web component of COMOS allows to upload and store arbitrary files at the webserver. This could allow an attacker to store malicious files.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37205	A vulnerability has been identified in SIMATIC Drive Controller family (All versions >= V2.9.2 < V2.9.4), SIMATIC ET 200SP Open Controller CPU 1515SP PC2 (incl. SIPLUS variants) (All versions >= V21.9 < V21.9.4), SIMATIC S7-1200 CPU family (incl. SIPLUS variants) (All versions >= V4.5.0 < V4.5.2), SIMATIC S7-1500 CPU family (incl. related ET200 CPUs and SIPLUS variants) (All versions >= V2.9.2 < V2.9.4), SIMATIC S7-1500 Software Controller (All versions >= V21.9 < V21.9.4), SIMATIC S7-PLCSIM Advanced (All versions >= V4.0 < V4.0 SP1), SIPLUS TIM 1531 IRC (All versions < V2.3.6), TIM 1531 IRC (All versions < V2.3.6). An unauthenticated attacker could cause a denial-of-service condition in a PLC when sending specially prepared packets over port 102/tcp. A restart of the affected device is needed to restore normal operations.	7.5	More Details
CVE-2021-45348	An Arbitrary File Deletion vulnerability exists in SourceCodester Attendance Management System v1.0 via the csv parameter in admin/pageUploadCSV.php, which can cause a Denial of Service (crash).	7.5	More Details
CVE-2021-45421	Emerson Dixell XWEB-500 products are affected by information disclosure via directory listing. A potential attacker can use this misconfiguration to access all the files in the remote directories. Note: the product has not been supported since 2018 and should be removed or replaced	7.5	More Details
CVE-2022-21698	client_golang is the instrumentation library for Go applications in Prometheus, and the promhttp package in client_golang provides tooling around HTTP servers and clients. In client_golang prior to version 1.11.1, HTTP server is susceptible to a Denial of Service through unbounded cardinality, and potential memory exhaustion, when handling requests with non-standard HTTP methods. In order to be affected, an instrumented software must use any of `promhttp.InstrumentHandler*` middleware except `RequestsInFlight`; not filter any specific methods (e.g GET) before middleware; pass metric with `method` label name to our middleware; and not have any firewall/LB/proxy that filters away requests with unknown `method`. client_golang version 1.11.1 contains a patch for this issue. Several workarounds are available, including removing the `method` label name from counter/gauge used in the InstrumentHandler; turning off affected promhttp handlers; adding custom middleware before promhttp handler that will sanitize the request method given by Go http.Request; and using a reverse proxy or web application firewall, configured to only allow a limited set of methods.	7.5	More Details
CVE-2019-25057	In Corda before 4.1, the meaning of serialized data can be modified via an attacker-controlled CustomSerializer.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0214	The Custom Popup Builder WordPress plugin before 1.3.1 autoload data from its popup on every pages, as such data can be sent by unauthenticated user, and is not validated in length, this could cause a denial of service on the blog	7.5	More Details
CVE-2022-21986	.NET Denial of Service Vulnerability	7.5	More Details
CVE-2022-21993	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability	7.5	More Details
CVE-2021-46462	njs through 0.7.1, used in NGINX, was discovered to contain a segmentation violation via njs_object_set_prototype in /src/njs_object.c.	7.5	More Details
CVE-2022-21965	Microsoft Teams Denial of Service Vulnerability	7.5	More Details
CVE-2022-0391	A flaw was found in Python, specifically within the urllib.parse module. This module helps break Uniform Resource Locator (URL) strings into components. The issue involves how the urlparse method does not sanitize input and allows characters like '\r' and '\n' in the URL path. This flaw allows an attacker to input a crafted URL, leading to injection attacks. This flaw affects Python versions prior to 3.10.0b1, 3.9.5, 3.8.11, 3.7.11 and 3.6.14.	7.5	More Details
CVE-2021-35380	A Directory Traversal vulnerability exists in Solari di Udine TermTalk Server (TTServer) 3.24.0.2, which lets an unauthenticated malicious user gain access to the files on the remote system by gaining access to the relative path of the file they want to download (http://url:port/file?valore).	7.5	More Details
CVE-2021-45347	An Incorrect Access Control vulnerability exists in zzcms 8.2, which lets a malicious user bypass authentication by changing the user name in the cookie to use any password.	7.5	More Details
CVE-2021-46354	Thinfinity VirtualUI 2.1.28.0, 2.1.32.1 and 2.5.26.2, fixed in version 3.0 is affected by an information disclosure vulnerability in the parameter "Addr" in cmd site. The ability to send requests to other systems can allow the vulnerable server to filtrate the real IP of the web server or increase the attack surface.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0538	Jenkins 2.333 and earlier, LTS 2.319.2 and earlier defines custom XStream converters that have not been updated to apply the protections for the vulnerability CVE-2021-43859 and allow unconstrained resource usage.	7.5	More Details
CVE-2021-4098	Insufficient data validation in Mojo in Google Chrome prior to 96.0.4664.110 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.	7.4	More Details
CVE-2022-23633	Action Pack is a framework for handling and responding to web requests. Under certain circumstances response bodies will not be closed. In the event a response is *not* notified of a `close`, `ActionDispatch::Executor` will not know to reset thread local state for the next request. This can lead to data being leaked to subsequent requests.This has been fixed in Rails 7.0.2.1, 6.1.4.5, 6.0.4.5, and 5.2.6.1. Upgrading is highly recommended, but to work around this problem a middleware described in GHSA-wh98-p28r-vrc9 can be used.	7.4	More Details
CVE-2022-22807	A CWE-1021 Improper Restriction of Rendered UI Layers or Frames vulnerability exists that could cause unintended modifications of the product settings or user accounts when deceiving the user to use the web interface rendered within iframes. Affected Product: EcoStruxure EV Charging Expert (formerly known as EVlink Load Management System): (HMIBSCEA53D1EDB, HMIBSCEA53D1EDS, HMIBSCEA53D1EDM, HMIBSCEA53D1EDL, HMIBSCEA53D1ESS, HMIBSCEA53D1ESM, HMIBSCEA53D1EML) (All Versions prior to SP8 (Version 01) V4.0.0.13)	7.4	More Details
CVE-2021-41441	A DoS attack in the web application of D-Link DIR-X1860 before v1.10WWB09_Beta allows a remote unauthenticated attacker to reboot the router via sending a specially crafted URL to an authenticated victim. The authenticated victim need to visit this URL, for the router to reboot.	7.4	More Details
CVE-2022-0016	An improper handling of exceptional conditions vulnerability exists within the Connect Before Logon feature of the Palo Alto Networks GlobalProtect app that enables a local attacker to escalate to SYSTEM or root privileges when authenticating with Connect Before Logon under certain circumstances. This issue impacts GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.9 on Windows and MacOS. This issue does not affect the GlobalProtect app on other platforms.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23622	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions there is a cross site scripting (XSS) vector in the `registerinline.vm` template related to the `xredirect` hidden field. This template is only used in the following conditions: 1. The wiki must be open to registration for anyone. 2. The wiki must be closed to view for Guest users or more specifically the XWiki.Registration page must be forbidden in View for guest user. A way to obtain the second condition is when administrators checked the "Prevent unregistered users from viewing pages, regardless of the page rights" box in the administration rights. This issue is patched in versions 12.10.11, 14.0-rc-1, 13.4.7, 13.10.3. There are two main ways for protecting against this vulnerability, the easiest and the best one is by applying a patch in the `registerinline.vm` template, the patch consists in checking the value of the xredirect field to ensure it matches: `<input type="hidden" name="xredirect" value="$escapetool.xml($!request.xredirect)" />`. If for some reason it's not possible to patch this file, another workaround is to ensure "Prevent unregistered users from viewing pages, regardless of the page rights" is not checked in the rights and apply a better right scheme using groups and rights on spaces.	7.4	More Details
CVE-2022-21957	Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability	7.2	More Details
CVE-2022-0557	OS Command Injection in Packagist microweber/microweber prior to 1.2.11.	7.2	More Details
CVE-2022-23048	Exponent CMS 2.6.0patch2 allows an authenticated admin user to upload a malicious extension in the format of a ZIP file with a PHP file inside it. After upload it, the PHP file will be placed at "themes/simpletheme/{rce}.php" from where can be accessed in order to execute commands.	7.2	More Details
CVE-2022-0588	Missing Authorization in Packagist librenms/librenms prior to 22.2.0.	7.1	More Details
CVE-2022-0580	Incorrect Authorization in Packagist librenms/librenms prior to 22.2.0.	7.1	More Details
CVE-2022-22292	Unprotected dynamic receiver in Telecom prior to SMR Feb-2022 Release 1 allows untrusted applications to launch arbitrary activity.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23273	Microsoft Dynamics GP Elevation Of Privilege Vulnerability	7.1	More Details
CVE-2022-21997	Windows Print Spooler Elevation of Privilege Vulnerability	7.1	More Details
CVE-2022-0017	An improper link resolution before file access ('link following') vulnerability exists in the Palo Alto Networks GlobalProtect app on Windows that enables a local attacker to disrupt system processes and potentially execute arbitrary code with SYSTEM privileges under certain circumstances. This issue impacts: GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.10 on Windows. GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.5 on Windows. This issue does not affect GlobalProtect app on other platforms.	7.0	More Details
CVE-2022-22766	Hardcoded credentials are used in specific BD Pyxis products. If exploited, threat actors may be able to gain access to the underlying file system and could potentially exploit application files for information that could be used to decrypt application credentials or gain access to electronic protected health information (ePHI) or other sensitive information.	7.0	More Details
CVE-2022-22717	Windows Print Spooler Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-22566	Select Dell Client Commercial and Consumer platforms contain a pre-boot direct memory access (DMA) vulnerability. An authenticated attacker with physical access to the system may potentially exploit this vulnerability in order to execute arbitrary code on the device.	6.9	More Details
CVE-2022-0020	A stored cross-site scripting (XSS) vulnerability in Palo Alto Network Cortex XSOAR web interface enables an authenticated network-based attacker to store a persistent javascript payload that will perform arbitrary actions in the Cortex XSOAR web interface on behalf of authenticated administrators who encounter the payload during normal operations. This issue impacts: All builds of Cortex XSOAR 6.1.0; Cortex XSOAR 6.2.0 builds earlier than build 1958888.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44850	On Xilinx Zynq-7000 SoC devices, physical modification of an SD boot image allows for a buffer overflow attack in the ROM. Because the Zynq-7000's boot image header is unencrypted and unauthenticated before use, an attacker can modify the boot header stored on an SD card so that a secure image appears to be unencrypted, and they will be able to modify the full range of register initialization values. Normally, these registers will be restricted when booting securely. Of importance to this attack are two registers that control the SD card's transfer type and transfer size. These registers could be modified a way that causes a buffer overflow in the ROM.	6.8	More Details
CVE-2022-20034	In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806.	6.8	More Details
CVE-2022-23620	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions AbstractSxExportURLFactoryActionHandler#processSx does not escape anything from SSX document references when serializing it on filesystem, it is possible to for the HTML export process to contain reference elements containing filesystem syntax like "../", "./". or "/" in general. The referenced elements are not properly escaped. This issue has been resolved in version 13.6-rc-1. This issue can be worked around by limiting or disabling document export.	6.8	More Details
CVE-2021-30324	Possible out of bound write due to lack of boundary check for the maximum size of buffer when sending a DCI packet to remote process in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	6.7	More Details
CVE-2022-20038	In ccu driver, there is a possible memory corruption due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183335; Issue ID: ALPS06183335.	6.7	More Details
CVE-2022-20039	In ccu driver, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06183345; Issue ID: ALPS06183345.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0111	NULL pointer dereference in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access.	6.7	More Details
CVE-2021-0169	Uncontrolled Search Path Element in software for Intel(R) PROSet/Wireless Wi-Fi in Windows 10 and 11 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-0167	Improper access control in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in Windows 10 and 11 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-0103	Insufficient control flow management in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access.	6.7	More Details
CVE-2021-0107	Unchecked return value in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2022-20030	In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793.	6.7	More Details
CVE-2021-0115	Buffer overflow in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-0118	Out-of-bounds read in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access.	6.7	More Details
CVE-2021-30325	Possible out of bound access of DCI resources due to lack of validation process and resource allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	6.7	More Details
CVE-2021-0168	Improper input validation in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0161	Improper input validation in firmware for Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and Killer(TM) Wi-Fi in Windows 10 and 11 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-0166	Exposure of Sensitive Information to an Unauthorized Actor in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow a privileged user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-0060	Insufficient compartmentalization in HECI subsystem for the Intel(R) SPS before versions SPS_E5_04.01.04.516.0, SPS_E5_04.04.04.033.0, SPS_E5_04.04.03.281.0, SPS_E5_03.01.03.116.0, SPS_E3_05.01.04.309.0, SPS_02.04.00.101.0, SPS_SoC-A_05.00.03.114.0, SPS_SoC-X_04.00.04.326.0, SPS_SoC-X_03.00.03.117.0, IGN_E5_91.00.00.167.0, SPS_PHI_03.01.03.078.0 may allow an authenticated user to potentially enable escalation of privilege via physical access.	6.6	More Details
CVE-2021-0125	Improper initialization in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via physical access.	6.6	More Details
CVE-2021-0124	Improper access control in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via physical access.	6.6	More Details
CVE-2022-25187	Jenkins Support Core Plugin 2.79 and earlier does not redact some sensitive information in the support bundle.	6.5	More Details
CVE-2022-25193	Missing permission checks in Jenkins Snow Commander Plugin 1.10 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified webserver using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2022-25197	Jenkins HashiCorp Vault Plugin 336.v182c0fbaaeb7 and earlier implements functionality that allows agent processes to read arbitrary files on the Jenkins controller file system.	6.5	More Details
CVE-2022-25201	Missing permission checks in Jenkins Checkmarx Plugin 2022.1.2 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified webserver using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25210	Jenkins Convertigo Mobile Platform Plugin 1.1 and earlier uses static fields to store job configuration information, allowing attackers with Item/Configure permission to capture passwords of the jobs that will be configured.	6.5	More Details
CVE-2022-23641	Discourse is an open source discussion platform. In versions prior to 2.8.1 in the `stable` branch, 2.9.0.beta2 in the `beta` branch, and 2.9.0.beta2 in the `tests-passed` branch, users can trigger a Denial of Service attack by posting a streaming URL. Parsing Oneboxes in the background job trigger an infinite loop, which cause memory leaks. This issue is patched in version 2.8.1 of the `stable` branch, 2.9.0.beta2 of the `beta` branch, and 2.9.0.beta2 of the `tests-passed` branch. As a workaround, disable onebox in admin panel completely or specify allow list of domains that will be oneboxed.	6.5	More Details
CVE-2022-23643	Sourcegraph is a code search and navigation engine. Sourcegraph versions 3.35 and 3.36 reintroduced a previously fixed side-channel vulnerabilitity in the Code Monitoring feature where strings in private source code could be guessed by an authenticated but unauthorized actor. This issue affects only the Code Monitoring feature, whereas CVE-2021-43823 also affected saved searches. A successful attack would require an authenticated bad actor to create many Code Monitors to receive confirmation that a specific string exists. This could allow an attacker to guess formatted tokens in source code, such as API keys. This issue was patched in versions 3.35.2 and 3.36.3 of Sourcegraph. Those who are unable to upgrade may disable the Code Monitor feature in their installation.	6.5	More Details
CVE-2021-45385	A Null Pointer Dereference vulnerability exits in ffjpeg d5cfd49 (2021-12-06) in bmp_load(). When the size information in metadata of the bmp is out of range, it returns without assign memory buffer to `pb->pdata` and did not exit the program. So the program crashes when it tries to access the pb->data, in jfif_encode() at jfif.c:763. This is due to the incomplete patch for CVE-2020-13438.	6.5	More Details
CVE-2021-46249	An authorization bypass exploited by a user-controlled key in SpecificApps REST API in ScratchOAuth2 before commit d856dc704b2504cd3b92cf089fdd366dd40775d6 allows app owners to set flags that indicate whether an app is verified on their own apps.	6.5	More Details
CVE-2020-13676	The QuickEdit module does not properly check access to fields in some circumstances, which can lead to unintended disclosure of field data. Sites are only affected if the QuickEdit module (which comes with the Standard profile) is installed.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25179	Jenkins Pipeline: Multibranch Plugin 706.vd43c65dec013 and earlier follows symbolic links to locations outside of the checkout directory for the configured SCM when reading files using the readTrusted step, allowing attackers able to configure Pipelines permission to read arbitrary files on the Jenkins controller file system.	6.5	More Details
CVE-2022-25186	Jenkins HashiCorp Vault Plugin 3.8.0 and earlier implements functionality that allows agent processes to retrieve any Vault secrets for use on the agent, allowing attackers able to control agent processes to obtain Vault secrets for an attacker-specified path and key.	6.5	More Details
CVE-2022-25184	Jenkins Pipeline: Build Step Plugin 2.15 and earlier reveals password parameter default values when generating a pipeline script using the Pipeline Snippet Generator, allowing attackers with Item/Read permission to retrieve the default password parameter value from jobs.	6.5	More Details
CVE-2021-39671	In code generated by aidl_const_expressions.cpp, there is a possible out of bounds read due to uninitialized data. This could lead to information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-206718630	6.5	More Details
CVE-2022-25178	Jenkins Pipeline: Shared Groovy Libraries Plugin 552.vd9cc05b8a2e1 and earlier does not restrict the names of resources passed to the libraryResource step, allowing attackers able to configure Pipelines permission to read arbitrary files on the Jenkins controller file system.	6.5	More Details
CVE-2022-0305	Inappropriate implementation in Service Worker API in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	6.5	More Details
CVE-2022-0108	Inappropriate implementation in Navigation in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2022-0109	Inappropriate implementation in Autofill in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to obtain potentially sensitive information via a crafted HTML page.	6.5	More Details
CVE-2022-0111	Inappropriate implementation in Navigation in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to incorrectly set origin via a crafted HTML page.	6.5	More Details
CVE-2022-0113	Inappropriate implementation in Blink in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0117	Policy bypass in Blink in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2022-0120	Inappropriate implementation in Passwords in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially leak cross-origin data via a malicious website.	6.5	More Details
CVE-2022-0291	Inappropriate implementation in Storage in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	6.5	More Details
CVE-2022-0292	Inappropriate implementation in Fenced Frames in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2022-0294	Inappropriate implementation in Push messaging in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.	6.5	More Details
CVE-2020-13674	The QuickEdit module does not properly validate access to routes, which could allow cross-site request forgery under some circumstances and lead to possible data integrity issues. Sites are only affected if the QuickEdit module (which comes with the Standard profile) is installed. Removing the "access in-place editing" permission from untrusted users will not fully mitigate the vulnerability.	6.5	More Details
CVE-2022-25177	Jenkins Pipeline: Shared Groovy Libraries Plugin 552.vd9cc05b8a2e1 and earlier follows symbolic links to locations outside of the expected Pipeline library when reading files using the libraryResource step, allowing attackers able to configure Pipelines to read arbitrary files on the Jenkins controller file system.	6.5	More Details
CVE-2022-24110	Kiteworks MFT 7.5 may allow an unauthorized user to reset other users' passwords. This is fixed in version 7.6 and later.	6.5	More Details
CVE-2021-39080	Due to weak obfuscation, IBM Cognos Analytics Mobile for Android application prior to version 1.1.14 , an attacker could be able to reverse engineer the codebase to gain knowledge about the programming technique, interface, class definitions, algorithms and functions used. IBM X-Force ID: 215593.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0579	Missing Authorization in Packagist snipe/snipe-it prior to 5.3.9.	6.5	More Details
CVE-2021-43941	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to modify several resources (including CsvFieldMappingsPage.jspa and ImporterValueMappingsPage.jspa) via a Cross-Site Request Forgery (CSRF) vulnerability in the jira-importers-plugin. The affected versions are before version 8.13.15, and from version 8.14.0 before 8.20.3.	6.5	More Details
CVE-2022-0587	Improper Authorization in Packagist librenms/librenms prior to 22.2.0.	6.5	More Details
CVE-2021-39665	In checkSpsUpdated of AAVCAssembler.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-204077881	6.5	More Details
CVE-2022-24684	HashiCorp Nomad and Nomad Enterprise 0.9.0 through 1.0.16, 1.1.11, and 1.2.5 allow operators with job-submit capabilities to use the spread stanza to panic server agents. Fixed in 1.0.18, 1.1.12, and 1.2.6.	6.5	More Details
CVE-2021-44960	In SVGPP SVG++ library 1.3.0, the XMLDocument::getRoot function in the renderDocument function handled the XMLDocument object improperly, returning a null pointer in advance at the second if, resulting in a null pointer reference behind the renderDocument function.	6.5	More Details
CVE-2022-25176	Jenkins Pipeline: Groovy Plugin 2648.va9433432b33c and earlier follows symbolic links to locations outside of the checkout directory for the configured SCM when reading the script file (typically Jenkinsfile) for Pipelines, allowing attackers able to configure Pipelines to read arbitrary files on the Jenkins controller file system.	6.5	More Details
CVE-2022-0309	Inappropriate implementation in Autofill in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.	6.5	More Details
CVE-2021-46252	A Cross-Site Request Forgery (CSRF) in RequirementsBypassPage.php of Scratch Wiki scratch-confirmaccount-v3 allows attackers to modify account request requirement bypasses.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22538	When a user opens a manipulated Adobe Illustrator file format (.ai, ai.x3d) received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9.0, the application crashes and becomes temporarily unavailable to the user until restart of the application. The file format details along with their CVE relevant information can be found below.	6.5	More Details
CVE-2022-22535	SAP ERP HCM Portugal - versions 600, 604, 608, does not perform necessary authorization checks for a report that reads the payroll data of employees in a certain area. Since the affected report only reads the payroll information, the attacker can neither modify any information nor cause availability impacts.	6.5	More Details
CVE-2021-0178	Improper input validation in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2022-0011	PAN-OS software provides options to exclude specific websites from URL category enforcement and those websites are blocked or allowed (depending on your rules) regardless of their associated URL category. This is done by creating a custom URL category list or by using an external dynamic list (EDL) in a URL Filtering profile. When the entries in these lists have a hostname pattern that does not end with a forward slash (/) or a hostname pattern that ends with an asterisk (*), any URL that starts with the specified pattern is considered a match. Entries with a caret (^) at the end of a hostname pattern match any top level domain. This may inadvertently allow or block more URLs than intended and allowing more URLs than intended represents a security risk. For example: example.com will match example.com.website.test example.com.* will match example.com.website.test example.com.^ will match example.com.test You should take special care when using such entries in policy rules that allow traffic. Where possible, use the exact list of hostname names ending with a forward slash (/) instead of using wildcards. PAN-OS 10.1 versions earlier than PAN-OS 10.1.3; PAN-OS 10.0 versions earlier than PAN-OS 10.0.8; PAN-OS 9.1 versions earlier than PAN-OS 9.1.12; all PAN-OS 9.0 versions; PAN-OS 8.1 versions earlier than PAN-OS 8.1.21, and Prisma Access 2.2 and 2.1 versions do not allow customers to change this behavior without changing the URL category list or EDL.	6.5	More Details
CVE-2021-0179	Improper Use of Validation Framework in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0183	Improper Validation of Specified Index, Position, or Offset in Input in software for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2021-33110	Improper input validation for some Intel(R) Wireless Bluetooth(R) products and Killer(TM) Bluetooth(R) products in Windows 10 and 11 before version 22.80 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2021-37613	Stormshield Network Security (SNS) 1.0.0 through 4.2.3 allows a Denial of Service.	6.5	More Details
CVE-2022-22537	When a user opens a manipulated Tagged Image File Format (.tiff, 2d.x3d)) received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9.0, the application crashes and becomes temporarily unavailable to the user until restart of the application. The file format details along with their CVE relevant information can be found below.	6.5	More Details
CVE-2021-3813	Improper Privilege Management in GitHub repository chatwoot/chatwoot prior to v2.2.	6.5	More Details
CVE-2021-0172	Improper input validation in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2022-22539	When a user opens a manipulated JPEG file format (.jpg, 2d.x3d) received from untrusted sources in SAP 3D Visual Enterprise Viewer - version 9.0, the application crashes and becomes temporarily unavailable to the user until restart of the application. The file format details along with their CVE relevant information can be found below.	6.5	More Details
CVE-2022-22542	S/4HANA Supplier Factsheet exposes the private address and bank details of an Employee Business Partner with Supplier Role, AND Enterprise Search for Customer, Supplier and Business Partner objects exposes the private address fields of Employee Business Partners, to an actor that is not explicitly authorized to have access to that information, which could compromise Confidentiality.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23617	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with edit right can copy the content of a page it does not have access to by using it as template of a new page. This issue has been patched in XWiki 13.2CR1 and 12.10.6. Users are advised to update. There are no known workarounds for this issue.	6.5	More Details
CVE-2021-45106	A vulnerability has been identified in SICAM TOOLBOX II (All versions). Affected applications use a circumventable access control within a database service. This could allow an attacker to access the database.	6.5	More Details
CVE-2022-23271	Microsoft Dynamics GP Elevation Of Privilege Vulnerability	6.5	More Details
CVE-2021-0177	Improper Validation of Consistency within input in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2021-33068	Null pointer dereference in subsystem for Intel(R) AMT before versions 15.0.35 may allow an authenticated user to potentially enable denial of service via network access.	6.5	More Details
CVE-2021-0173	Improper Validation of Consistency within input in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow a unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2021-0174	Improper Use of Validation Framework in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow a unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2021-38679	An improper authentication vulnerability has been reported to affect QNAP NAS running Kazoo Server. If exploited, this vulnerability allows attackers to compromise the security of the system. We have already fixed this vulnerability in the following versions of Kazoo Server: Kazoo Server 4.11.22 and later	6.5	More Details
CVE-2021-0165	Improper input validation in firmware for Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-0175	Improper Validation of Specified Index, Position, or Offset in Input in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2022-23432	An improper input validation in SMC_SRPMB_WSM handler of RPMB ldfw prior to SMR Feb-2022 Release 1 allows arbitrary memory write and code execution.	6.4	More Details
CVE-2021-25115	The WP Photo Album Plus WordPress plugin before 8.0.10 was vulnerable to Stored Cross-Site Scripting (XSS). Error log content was handled improperly, therefore any user, even unauthenticated, could cause arbitrary javascript to be executed in the admin panel.	6.4	More Details
CVE-2022-23431	An improper boundary check in RPMB ldfw prior to SMR Feb-2022 Release 1 allows arbitrary memory write and code execution.	6.4	More Details
CVE-2022-23628	OPA is an open source, general-purpose policy engine. Under certain conditions, pretty-printing an abstract syntax tree (AST) that contains synthetic nodes could change the logic of some statements by reordering array literals. Example of policies impacted are those that parse and compare web paths. **All of these** three conditions have to be met to create an adverse effect: 1. An AST of Rego had to be **created programmatically** such that it ends up containing terms without a location (such as wildcard variables). 2. The AST had to be **pretty-printed** using the `github.com/open-policy-agent/opa/format` package. 3. The result of the pretty-printing had to be **parsed and evaluated again** via an OPA instance using the bundles, or the Golang packages. If any of these three conditions are not met, you are not affected. Notably, all three would be true if using **optimized bundles**, i.e. bundles created with `opa build -O=1` or higher. In that case, the optimizer would fulfil condition (1.), the result of that would be pretty-printed when writing the bundle to disk, fulfilling (2.). When the bundle was then used, we'd satisfy (3.). As a workaround users may disable optimization when creating bundles.	6.3	More Details
CVE-2022-0586	Infinite loop in RTMPT protocol dissector in Wireshark 3.6.0 to 3.6.1 and 3.4.0 to 3.4.11 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2022-0583	Crash in the PVFS protocol dissector in Wireshark 3.6.0 to 3.6.1 and 3.4.0 to 3.4.11 allows denial of service via packet injection or crafted capture file	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0582	Unaligned access in the CSN.1 protocol dissector in Wireshark 3.6.0 to 3.6.1 and 3.4.0 to 3.4.11 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2022-0581	Crash in the CMS protocol dissector in Wireshark 3.6.0 to 3.6.1 and 3.4.0 to 3.4.11 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2022-23998	Improper access control vulnerability in Camera prior to versions 11.1.02.16 in Android R(11), 10.5.03.77 in Android Q(10) and 9.0.6.68 in Android P(9) allows untrusted applications to take a picture in screenlock status.	6.2	More Details
CVE-2022-23638	svg-sanitizer is a SVG/XML sanitizer written in PHP. A cross-site scripting vulnerability impacts all users of the `svg-sanitizer` library prior to version 0.15.0. This issue is fixed in version 0.15.0. There is currently no workaround available.	6.2	More Details
CVE-2021-0119	Improper initialization in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via physical access.	6.2	More Details
CVE-2021-43106	A Header Injection vulnerability exists in Compass Plus TranzWare Online FIMI Web Interface Tranzware Online (TWO) 5.3.33.3 F38 and FIMI 4.2.19.4 25.The HTTP host header can be manipulated and cause the application to behave in unexpected ways. Any changes made to the header would just cause the request to be sent to a completely different Domain/IP address. This is due to that the server implicitly trusts the Host header, and fails to validate or escape it properly. An attacker can use this input to redirect target users to a malicious domain/web page. This would result in expanding the potential to further attacks and malicious actions.	6.1	More Details
CVE-2022-0208	The MapPress Maps for WordPress plugin before 2.73.4 does not sanitise and escape the mapid parameter before outputting it back in the "Bad mapid" error message, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-24227	A cross-site scripting (XSS) vulnerability in BoltWire v7.10 and v 8.00 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the name and lastname parameters.	6.1	More Details
CVE-2022-0597	Open Redirect in Packagist microweber/microweber prior to 1.2.11.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23367	Fulusso v1.1 was discovered to contain a DOM-based cross-site scripting (XSS) vulnerability in /BindAccount/SuccessTips.js. This vulnerability allows attackers to inject malicious code into a victim user's device via open redirection.	6.1	More Details
CVE-2021-25033	The WordPress Newsletter Plugin WordPress plugin before 1.6.5 does not validate the to parameter before redirecting the user to its given value, leading to an open redirect issue	6.1	More Details
CVE-2022-0212	The SpiderCalendar WordPress plugin through 1.5.65 does not sanitise and escape the callback parameter before outputting it back in the page via the window AJAX action (available to both unauthenticated and authenticated users), leading to a Reflected Cross-Site Scripting issue.	6.1	More Details
CVE-2021-25107	The Form Store to DB WordPress plugin before 1.1.1 does not sanitise and escape parameter keys before outputting it back in the created entry, allowing unauthenticated attacker to perform Cross-Site Scripting attacks against admin	6.1	More Details
CVE-2022-0201	The Permalink Manager Lite WordPress plugin before 2.2.15 and Permalink Manager Pro WordPress plugin before 2.2.15 do not sanitise and escape query parameters before outputting them back in the debug page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2022-0206	The NewStatPress WordPress plugin before 1.3.6 does not properly escape the whatX parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2022-23391	A cross-site scripting (XSS) vulnerability in Pybbs v6.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload inserted into the Search box.	6.1	More Details
CVE-2022-0576	Cross-site Scripting (XSS) - Generic in Packagist librenms/librenms prior to 22.1.0.	6.1	More Details
CVE-2022-22534	Due to insufficient encoding of user input, SAP NetWeaver allows an unauthenticated attacker to inject code that may expose sensitive data like user ID and password. These endpoints are normally exposed over the network and successful exploitation can partially impact confidentiality of the application.	6.1	More Details
CVE-2022-0176	The PowerPack Lite for Beaver Builder WordPress plugin before 1.2.9.3 does not sanitise and escape the tab parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0193	The Complianz WordPress plugin before 6.0.0 does not escape the s parameter before outputting it back in an attribute in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2020-13672	Cross-site Scripting (XSS) vulnerability in Drupal core's sanitization API fails to properly filter cross-site scripting under certain circumstances. This issue affects: Drupal Core 9.1.x versions prior to 9.1.7; 9.0.x versions prior to 9.0.12; 8.9.x versions prior to 8.9.14; 7.x versions prior to 7.80.	6.1	More Details
CVE-2022-23637	K-Box is a web-based application to manage documents, images, videos and geodata. Prior to version 0.33.1, a stored Cross-Site-Scripting (XSS) vulnerability is present in the markdown editor used by the document abstract and markdown file preview. A specifically crafted anchor link can, if clicked, execute untrusted javascript actions, like retrieving user cookies. Version 0.33.1 includes a patch that allows discarding unsafe links.	6.1	More Details
CVE-2021-24874	The Newsletter, SMTP, Email marketing and Subscribe forms by Sendinblue WordPress plugin before 3.1.31 does not escape the lang and pid parameter before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2020-13673	The Entity Embed module provides a filter to allow embedding entities in content fields. In certain circumstances, the filter could allow an unprivileged user to inject HTML into a page when it is accessed by a trusted user with permission to embed entities. In some cases, this could lead to cross-site scripting.	6.1	More Details
CVE-2022-0571	Cross-site Scripting (XSS) - Reflected in GitHub repository phoronix-test-suite/phoronix-test-suite prior to 10.8.2.	6.1	More Details
CVE-2021-46251	A reflected cross-site scripting (XSS) in ScratchOAuth2 before commit 1603f04e44ef67dde6ccffe866d2dca16defb293 allows attackers to execute arbitrary web scripts or HTML via a crafted POST request.	6.1	More Details
CVE-2022-0527	Cross-site Scripting (XSS) - Stored in GitHub repository chatwoot/chatwoot prior to 2.2.0.	6.1	More Details
CVE-2022-24682	An issue was discovered in the Calendar feature in Zimbra Collaboration Suite 8.8.x before 8.8.15 patch 30 (update 1), as exploited in the wild starting in December 2021. An attacker could place HTML containing executable JavaScript inside element attributes. This markup becomes unescaped, causing arbitrary markup to be injected into the document.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0526	Cross-site Scripting (XSS) - Stored in GitHub repository chatwoot/chatwoot prior to 2.2.0.	6.1	More Details
CVE-2022-22812	A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could cause a web session compromise when an attacker injects and then executes arbitrary malicious JavaScript code inside the target browser. Affected Product: spaceLYnk (V2.6.2 and prior), Wiser for KNX (formerly homeLYnk) (V2.6.2 and prior), fellerLYnk (V2.6.2 and prior)	6.1	More Details
CVE-2022-0018	An information exposure vulnerability exists in the Palo Alto Networks GlobalProtect app on Windows and MacOS where the credentials of the local user account are sent to the GlobalProtect portal when the Single Sign-On feature is enabled in the GlobalProtect portal configuration. This product behavior is intentional and poses no security risk when connecting to trusted GlobalProtect portals configured to use the same Single Sign-On credentials both for the local user account as well as the GlobalProtect login. However when the credentials are different, the local account credentials are inadvertently sent to the GlobalProtect portal for authentication. A third party MITM type of attacker cannot see these credentials in transit. This vulnerability is a concern where the GlobalProtect app is deployed on Bring-your-Own-Device (BYOD) type of clients with private local user accounts or GlobalProtect app is used to connect to different organizations. Fixed versions of GlobalProtect app have an app setting to prevent the transmission of the user's local user credentials to the target GlobalProtect portal regardless of the portal configuration. This issue impacts: GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.10 on Windows and MacOS; GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.9 on Windows and MacOS This issue does not affect GlobalProtect app on other platforms.	6.1	More Details
CVE-2022-23102	A vulnerability has been identified in SINEMA Remote Connect Server (All versions < V2.0). Affected products contain an open redirect vulnerability. An attacker could trick a valid authenticated user to the device into clicking a malicious link there by leading to phishing attacks.	6.1	More Details
CVE-2022-23312	A vulnerability has been identified in Spectrum Power 4 (All versions < V4.70 SP9 Security Patch 1). The integrated web application "Online Help" in affected product contains a Cross-Site Scripting (XSS) vulnerability that could be exploited if unsuspecting users are tricked into accessing a malicious link.	6.1	More Details
CVE-2021-45357	Cross Site Scripting (XSS) vulnerability exists in Piwigo 12.x via the pwg_activity function in include/functions.inc.php.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0560	Open Redirect in Packagist microweber/microweber prior to 1.2.11.	6.1	More Details
CVE-2021-31814	In Stormshield 1.1.0, and 2.1.0 through 2.9.0, an attacker can block a client from accessing the VPN and can obtain sensitive information through the SN VPN SSL Client.	6.1	More Details
CVE-2021-41445	A reflected cross-site-scripting attack in web application of D-Link DIR-X1860 before v1.10WWB09_Beta allows a remote unauthenticated attacker to execute code in the device of the victim via sending a specific URL to the unauthenticated victim.	6.1	More Details
CVE-2020-13668	Access Bypass vulnerability in Drupal Core allows for an attacker to leverage the way that HTML is rendered for affected forms in order to exploit the vulnerability. This issue affects: Drupal Core 8.8.x versions prior to 8.8.10; 8.9.x versions prior to 8.9.6; 9.0.x versions prior to 9.0.6.	6.1	More Details
CVE-2020-13669	Cross-site Scripting (XSS) vulnerability in ckeditor of Drupal Core allows attacker to inject XSS. This issue affects: Drupal Core 8.8.x versions prior to 8.8.10.; 8.9.x versions prior to 8.9.6; 9.0.x versions prior to 9.0.6.	6.1	More Details
CVE-2022-24589	Burden v3.0 was discovered to contain a stored cross-site scripting (XSS) in the Add Category function. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the task parameter.	6.1	More Details
CVE-2022-23255	Microsoft OneDrive for Android Security Feature Bypass Vulnerability	5.9	More Details
CVE-2022-24320	A CWE-295: Improper Certificate Validation vulnerability exists that could allow a Man-in-theMiddle attack when communications between the client and Geo SCADA database server are intercepted. Affected Product: ClearSCADA (All Versions), EcoStruxure Geo SCADA Expert 2019 (All Versions), EcoStruxure Geo SCADA Expert 2020 (All Versions)	5.9	More Details
CVE-2022-24968	In Mellium mellium.im/xmpp through 0.21.0, an attacker capable of spoofing DNS TXT records can redirect a WebSocket connection request to a server under their control without causing TLS certificate verification to fail. This occurs because the wrong host name is selected during this verification.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24319	A CWE-295: Improper Certificate Validation vulnerability exists that could allow a Man-in-theMiddle attack when communications between the client and Geo SCADA web server are intercepted. Affected Product: ClearSCADA (All Versions), EcoStruxure Geo SCADA Expert 2019 (All Versions), EcoStruxure Geo SCADA Expert 2020 (All Versions)	5.9	More Details
CVE-2022-24686	HashiCorp Nomad and Nomad Enterprise 0.3.0 through 1.0.17, 1.1.11, and 1.2.5 artifact download functionality has a race condition such that the Nomad client agent could download the wrong artifact into the wrong destination. Fixed in 1.0.18, 1.1.12, and 1.2.6	5.9	More Details
CVE-2022-20738	A vulnerability in the Cisco Umbrella Secure Web Gateway service could allow an unauthenticated, remote attacker to bypass the file inspection feature. This vulnerability is due to insufficient restrictions in the file inspection feature. An attacker could exploit this vulnerability by downloading a crafted payload through specific methods. A successful exploit could allow the attacker to bypass file inspection protections and download a malicious payload.	5.8	More Details
CVE-2021-3398	Stormshield Network Security (SNS) 3.x has an Integer Overflow in the high-availability component.	5.8	More Details
CVE-2021-33114	Improper input validation for some Intel(R) PROSet/Wireless WiFi in multiple operating systems and Killer(TM) WiFi in Windows 10 and 11 may allow an authenticated user to potentially enable denial of service via adjacent access.	5.7	More Details
CVE-2021-33139	Improper conditions check in firmware for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products before version 22.100 may allow an authenticated user to potentially enable denial of service via adjacent access.	5.7	More Details
CVE-2022-24926	Improper input validation vulnerability in SmartTagPlugin prior to version 1.2.15-6 allows privileged attackers to trigger a XSS on a victim's devices.	5.7	More Details
CVE-2021-33155	Improper input validation in firmware for some Intel(R) Wireless Bluetooth(R) and Killer(TM) Bluetooth(R) products before version 22.100 may allow an authenticated user to potentially enable denial of service via adjacent access.	5.7	More Details
CVE-2022-22712	Windows Hyper-V Denial of Service Vulnerability	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33147	Improper conditions check in the Intel(R) IPP Crypto library before version 2021.2 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2021-33105	Out-of-bounds read in some Intel(R) Core(TM) processors with Radeon(TM) RX Vega M GL integrated graphics before version 21.10 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2021-0076	Improper Validation of Specified Index, Position, or Offset in Input in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow a privileged user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-33166	Incorrect default permissions for the Intel(R) RXT for Chromebook application, all versions, may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2021-33119	Improper access control in the Intel(R) RealSense(TM) DCM before version 20210625 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2021-37107	There is an improper memory access permission configuration on ACPU.Successful exploitation of this vulnerability may cause out-of-bounds access.	5.5	More Details
CVE-2021-37115	There is an unauthorized rewriting vulnerability with the memory access management module on ACPU.Successful exploitation of this vulnerability may affect service confidentiality.	5.5	More Details
CVE-2021-39986	There is an unauthorized rewriting vulnerability with the memory access management module on ACPU.Successful exploitation of this vulnerability may affect service confidentiality.	5.5	More Details
CVE-2021-39666	In extract of MediaMetricsItem.h, 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.Product: AndroidVersions: Android-11 Android-12Android ID: A-204445255	5.5	More Details
CVE-2021-0145	Improper initialization of shared resources in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33096	Improper isolation of shared resources in network on chip for the Intel(R) 82599 Ethernet Controllers and Adapters may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-33061	Insufficient control flow management for the Intel(R) 82599 Ethernet Controllers and Adapters may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2021-39664	In LoadedPackage::Load of LoadedArsc.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure when parsing an APK file with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-203938029	5.5	More Details
CVE-2021-39631	In clear_data_dlg_text of strings.xml, there is a possible situation when "Clear storage" functionality sets up the wrong security/privacy expectations due to a misleading message. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-193890833	5.5	More Details
CVE-2021-0127	Insufficient control flow management in some Intel(R) Processors may allow an authenticated user to potentially enable a denial of service via local access.	5.5	More Details
CVE-2021-0072	Improper input validation in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow a privileged user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2021-44879	In gc_data_segment in fs/f2fs/gc.c in the Linux kernel before 5.16.3, special files are not considered, leading to a move_data_page NULL pointer dereference.	5.5	More Details
CVE-2021-0170	Exposure of Sensitive Information to an Unauthorized Actor in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2021-0171	Improper access control in software for Intel(R) PROSet/Wireless Wi-Fi and Killer(TM) Wi-Fi in Windows 10 and 11 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24959	An issue was discovered in the Linux kernel before 5.16.5. There is a memory leak in yam_siocdevprivate in drivers/net/hamradio/yam.c.	5.5	More Details
CVE-2021-0524	In isServiceDistractionOptimized of CarPackageManagerService.java, there is a possible disclosure of installed packages due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-180418334	5.5	More Details
CVE-2021-45387	tcpreplay 4.3.4 has a Reachable Assertion in add_tree_ipv4() at tree.c.	5.5	More Details
CVE-2021-45386	tcpreplay 4.3.4 has a Reachable Assertion in add_tree_ipv6() at tree.c	5.5	More Details
CVE-2021-45402	The check_alu_op() function in kernel/bpf/verifier.c in the Linux kernel through v5.16-rc5 did not properly update bounds while handling the mov32 instruction, which allows local users to obtain potentially sensitive address information, aka a "pointer leak."	5.5	More Details
CVE-2021-39991	There is an unauthorized rewriting vulnerability with the memory access management module on ACPU.Successful exploitation of this vulnerability may affect service confidentiality.	5.5	More Details
CVE-2022-21998	Windows Common Log File System Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2021-40045	There is a vulnerability of signature verification mechanism failure in system upgrade through recovery mode.Successful exploitation of this vulnerability may affect service confidentiality.	5.5	More Details
CVE-2022-20042	In Bluetooth, there is a possible information disclosure due to incorrect error handling. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108487; Issue ID: ALPS06108487.	5.5	More Details
CVE-2022-22291	Logging of excessive data vulnerability in telephony prior to SMR Feb-2022 Release 1 allows privileged attackers to get Cell Location Information through log of user device.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0562	Null source pointer passed as an argument to memcpy() function within TIFFReadDirectory() in tif_dirread.c in libtiff versions from 4.0 to 4.3.0 could lead to Denial of Service via crafted TIFF file. For users that compile libtiff from sources, a fix is available with commit 561599c.	5.5	More Details
CVE-2022-0561	Null source pointer passed as an argument to memcpy() function within TIFFFetchStripThing() in tif_dirread.c in libtiff versions from 3.9.0 to 4.3.0 could lead to Denial of Service via crafted TIFF file. For users that compile libtiff from sources, the fix is available with commit eecb0712.	5.5	More Details
CVE-2022-23252	Microsoft Office Information Disclosure Vulnerability	5.5	More Details
CVE-2022-0382	An information leak flaw was found due to uninitialized memory in the Linux kernel's TIPC protocol subsystem, in the way a user sends a TIPC datagram to one or more destinations. This flaw allows a local user to read some kernel memory. This issue is limited to no more than 7 bytes, and the user cannot control what is read. This flaw affects the Linux kernel versions prior to 5.17-rc1.	5.5	More Details
CVE-2022-21985	Windows Remote Access Connection Manager Information Disclosure Vulnerability	5.5	More Details
CVE-2022-22716	Microsoft Excel Information Disclosure Vulnerability	5.5	More Details
CVE-2022-22710	Windows Common Log File System Driver Denial of Service Vulnerability	5.5	More Details
CVE-2022-21226	Out-of-bounds read in the Intel(R) Trace Analyzer and Collector before version 2021.5 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-21218	Uncaught exception in the Intel(R) Trace Analyzer and Collector before version 2021.5 may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-21157	Improper access control in the Intel(R) Smart Campus Android application before version 6.1 may allow authenticated user to potentially enable information disclosure via local access.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21156	Access of uninitialized pointer in the Intel(R) Trace Analyzer and Collector before version 2021.5 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2022-21153	Improper access control in the Intel(R) Capital Global Summit Android application may allow an authenticated user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2022-21133	Out-of-bounds read in the Intel(R) Trace Analyzer and Collector before version 2021.5 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2022-20046	In Bluetooth, there is a possible memory corruption due to a logic error. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06142410; Issue ID: ALPS06142410.	5.5	More Details
CVE-2021-39687	In HandleTransactionIoEvent of actuator_driver.cc, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-204421047References: N/A	5.5	More Details
CVE-2022-20036	In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171689; Issue ID: ALPS06171689.	5.5	More Details
CVE-2022-22002	Windows User Account Profile Picture Denial of Service Vulnerability	5.5	More Details
CVE-2021-39688	In TBD of TBD, there is a possible out of bounds read due to TBD. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-206039140References: N/A	5.5	More Details
CVE-2022-20017	In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862991; Issue ID: ALPS05862991.	5.5	More Details
CVE-2022-0534	A vulnerability was found in htmldoc version 1.9.15 where the stack out-of-bounds read takes place in gif_get_code() and occurs when opening a malicious GIF file, which can result in a crash (segmentation fault).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20037	In ion driver, there is a possible information disclosure due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171705; Issue ID: ALPS06171705.	5.5	More Details
CVE-2022-23621	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with SCRIPT right can read any file located in the XWiki WAR (for example xwiki.cfg and xwiki.properties) through XWiki#invokeServletAndReturnAsString as `$xwiki.invokeServletAndReturnAsString("/WEB-INF/xwiki.cfg")`. This issue has been patched in XWiki versions 12.10.9, 13.4.3 and 13.7-rc-1. Users are advised to update. The only workaround is to limit SCRIPT right.	5.5	More Details
CVE-2022-0530	A flaw was found in Unzip. The vulnerability occurs during the conversion of a wide string to a local string that leads to a heap of out-of-bound write. This flaw allows an attacker to input a specially crafted zip file, leading to a crash or code execution.	5.5	More Details
CVE-2022-0529	A flaw was found in Unzip. The vulnerability occurs during the conversion of a wide string to a local string that leads to a heap of out-of-bound write. This flaw allows an attacker to input a specially crafted zip file, leading to a crash or code execution.	5.5	More Details
CVE-2022-23269	Microsoft Dynamics GP Spoofing Vulnerability	5.4	More Details
CVE-2022-0575	Cross-site Scripting (XSS) - Stored in Packagist librenms/librenms prior to 22.2.0.	5.4	More Details
CVE-2022-24588	Flatpress v1.2.1 was discovered to contain a cross-site scripting (XSS) vulnerability in the Upload SVG File function.	5.4	More Details
CVE-2021-46557	Vicidial 2.14-783a was discovered to contain a cross-site scripting (XSS) vulnerability via the input tabs.	5.4	More Details
CVE-2022-24586	A stored cross-site scripting (XSS) vulnerability in the component /core/admin/categories.php of PluXml v5.8.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the content and thumbnail parameters.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24587	A stored cross-site scripting (XSS) vulnerability in the component core/admin/medias.php of PluXml v5.8.7 allows attackers to execute arbitrary web scripts or HTML.	5.4	More Details
CVE-2022-24585	A stored cross-site scripting (XSS) vulnerability in the component /core/admin/comment.php of PluXml v5.8.7 allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the author parameter.	5.4	More Details
CVE-2021-46558	Multiple cross-site scripting (XSS) vulnerabilities in the Add User module of Issabel PBX 20200102 allows attackers to execute arbitrary web scripts or HTML via a crafted payload inserted into the username and password fields.	5.4	More Details
CVE-2022-25203	Jenkins Team Views Plugin 0.9.0 and earlier does not escape team names, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Overall/Read permission.	5.4	More Details
CVE-2022-0589	Cross-site Scripting (XSS) - Stored in Packagist librenms/librenms prior to 22.1.0.	5.4	More Details
CVE-2022-23615	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions any user with SCRIPT right can save a document with the right of the current user which allow accessing API requiring programming right if the current user has programming right. This has been patched in XWiki 13.0. Users are advised to update to resolve this issue. The only known workaround is to limit SCRIPT access.	5.4	More Details
CVE-2021-39079	IBM Cognos Analytics Mobile for Android applications prior to version 1.1.14 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 215592.	5.4	More Details
CVE-2021-44912	In XE 1.116, when uploading the Normal button, there is no restriction on the file suffix, which leads to any file uploading to the files directory. Since .htaccess only restricts the PHP type, uploading HTML-type files leads to stored XSS vulnerabilities. If the .htaccess configuration is improper, for example before the XE 1.11.2 version, you can upload the PHP type file to GETSHELL.	5.4	More Details
CVE-2022-23378	A Cross-Site Scripting (XSS) vulnerability exists within the 3.2.2 version of TastyIgniter. The "items%5B0%5D%5Bpath%5D" parameter of a request made to /admin/allergens/edit/1 is vulnerable.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44911	XE before 1.11.6 is vulnerable to Unrestricted file upload via modules/menu/menu.admin.controller.php. When uploading the Mouse over button and When selected button, there is no restriction on the file suffix, which leads to any file uploading to the files directory. Since .htaccess only restricts the PHP type, uploading HTML-type files leads to stored XSS vulnerabilities.	5.4	More Details
CVE-2022-25196	Jenkins GitLab Authentication Plugin 1.13 and earlier records the HTTP Referer header as part of the URL query parameters when the authentication process starts, allowing attackers with access to Jenkins to craft a URL that will redirect users to an attacker-specified URL after logging in.	5.4	More Details
CVE-2022-25204	Jenkins Doktor Plugin 0.4.1 and earlier implements functionality that allows agent processes to render files on the controller as Markdown or Asciidoc, and error messages allow attackers able to control agent processes to determine whether a file with a given name exists.	5.4	More Details
CVE-2022-21818	NVIDIA License System contains a vulnerability in the installation scripts for the DLS virtual appliance, where a user on a network after signing in to the portal can access other users' credentials, allowing them to gain escalated privileges, resulting in limited impact to both confidentiality and integrity.	5.4	More Details
CVE-2022-25185	Jenkins Generic Webhook Trigger Plugin 1.81 and earlier does not escape the build cause when using the webhook, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-25189	Jenkins Custom Checkbox Parameter Plugin 1.1 and earlier does not escape parameter names of custom checkbox parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-25191	Jenkins Agent Server Parameter Plugin 1.0 and earlier does not escape parameter names of agent server parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2022-24590	A stored cross-site scripting (XSS) vulnerability in the Add Link function of BackdropCMS v1.21.1 allows attackers to execute arbitrary web scripts or HTML.	5.4	More Details
CVE-2022-0539	Cross-site Scripting (XSS) - Stored in Packagist ptrofimov/beanstalk_console prior to 1.7.14.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25018	The PPOM for WooCommerce WordPress plugin before 24.0 does not have authorisation and CSRF checks in the ppom_settings_panel_action AJAX action, allowing any authenticated to call it and set arbitrary settings. Furthermore, due to the lack of sanitisation and escaping, it could lead to Stored XSS issues	5.4	More Details
CVE-2021-4046	The m_txtNom y m_txtCognoms parameters in TCMAN GIM v8.01 allow an attacker to perform persistent XSS attacks. This vulnerability could be used to carry out a number of browser-based attacks including browser hijacking or theft of sensitive data.	5.4	More Details
CVE-2021-33120	Out of bounds read under complex microarchitectural condition in memory subsystem for some Intel Atom(R) Processors may allow authenticated user to potentially enable information disclosure or cause denial of service via network access.	5.4	More Details
CVE-2022-22546	Due to improper HTML encoding in input control summary, an authorized attacker can execute XSS vulnerability in SAP Business Objects Web Intelligence (BI Launchpad) - version 420.	5.4	More Details
CVE-2021-46355	OCS Inventory 2.9.1 is affected by Cross Site Scripting (XSS). To exploit the vulnerability, the attacker needs to manipulate the name of some device on your computer, such as a printer, replacing the device name with some malicious code that allows the execution of Stored Cross-site Scripting (XSS).	5.4	More Details
CVE-2021-44970	MiniCMS v1.11 was discovered to contain a cross-site scripting (XSS) vulnerability via /mc-admin/page-edit.php.	5.4	More Details
CVE-2022-0200	Themify Portfolio Post WordPress plugin before 1.1.7 does not sanitise and escape the num_of_pages parameter before outputting it back the response of the themify_create_popup_page_pagination AJAX action (available to any authenticated user), leading to a Reflected Cross-Site Scripting	5.4	More Details
CVE-2022-23707	An XSS vulnerability was found in Kibana index patterns. Using this vulnerability, an authenticated user with permissions to create index patterns can inject malicious javascript into the index pattern which could execute against other users	5.4	More Details
CVE-2021-24446	The Remove Footer Credit WordPress plugin before 1.0.6 does not have CSRF check in place when saving its settings, which could allow attacker to make logged in admins change them and lead to Stored XSS issue as well due to the lack of sanitisation	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0558	Cross-site Scripting (XSS) - Stored in Packagist microweber/microweber prior to 1.2.11.	5.4	More Details
CVE-2022-23049	Exponent CMS 2.6.0patch2 allows an authenticated user to inject persistent JavaScript code on the "User-Agent" header when logging in. When an administrator user visits the "User Sessions" tab, the JavaScript will be triggered allowing an attacker to compromise the administrator session.	5.4	More Details
CVE-2021-45286	Directory Traversal vulnerability exists in ZZCMS 2021 via the skin parameter in 1) index.php, 2) bottom.php, and 3) top_index.php.	5.3	More Details
CVE-2022-23280	Microsoft Outlook for Mac Security Feature Bypass Vulnerability	5.3	More Details
CVE-2021-45310	Sangoma Technologies Corporation Switchvox Version 102409 is affected by an information disclosure vulnerability due to an improper access restriction. Users information such as first name, last name, acount id, server uuid, email address, profile image, number, timestamps, etc can be extracted by sending an unauthenticated HTTP GET request to the https://Switchvox-IP/main?cmd=invalid_browser.	5.3	More Details
CVE-2022-23429	An improper boundary check in audio hal service prior to SMR Feb-2022 Release 1 allows attackers to read invalid memory and it leads to application crash.	5.3	More Details
CVE-2022-22809	A CWE-306: Missing Authentication for Critical Function vulnerability exists that could allow modifications of the touch configurations in an unauthorized manner when an attacker attempts to modify the touch configurations. Affected Product: spaceLYnk (V2.6.2 and prior), Wiser for KNX (formerly homeLYnk) (V2.6.2 and prior), fellerLYnk (V2.6.2 and prior)	5.3	More Details
CVE-2022-0569	Observable Discrepancy in Packagist snipe/snipe-it prior to v5.3.9.	5.3	More Details
CVE-2022-23619	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible to guess if a user has an account on the wiki by using the "Forgot your password" form, even if the wiki is closed to guest users. This problem has been patched on XWiki 12.10.9, 13.4.1 and 13.6RC1. Users are advised yo update. There are no known workarounds for this issue.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45901	The password-reset form in ServiceNow Orlando provides different responses to invalid authentication attempts depending on whether the username exists.	5.3	More Details
CVE-2022-24111	In Mahara 21.04 before 21.04.3 and 21.10 before 21.10.1, portfolios created in groups that have not been shared with non-group members and portfolios created on the site and institution levels can be viewed without requiring a login if the URL to these portfolios is known.	5.3	More Details
CVE-2022-0512	Authorization Bypass Through User-Controlled Key in NPM url-parse prior to 1.5.6.	5.3	More Details
CVE-2021-42000	When a password reset or password change flow with an authentication policy is configured and the adapter in the reset or change policy supports multiple parallel reset flows, an existing user can reset another existing users password.	5.3	More Details
CVE-2022-0188	The CMP WordPress plugin before 4.0.19 allows any user, even not logged in, to arbitrarily change the coming soon page layout.	5.3	More Details
CVE-2022-23254	Microsoft Power BI Information Disclosure Vulnerability	4.9	More Details
CVE-2022-22545	A high privileged user who has access to transaction SM59 can read connection details stored with the destination for http calls in SAP NetWeaver Application Server ABAP and ABAP Platform - versions 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756.	4.9	More Details
CVE-2022-23047	Exponent CMS 2.6.0patch2 allows an authenticated admin user to inject persistent JavaScript code inside the "Site/Organization Name","Site Title" and "Site Header" parameters while updating the site settings on "/exponentcms/administration/configure_site"	4.8	More Details
CVE-2022-25202	Jenkins Promoted Builds (Simple) Plugin 1.9 and earlier does not escape the name of custom promotion levels, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Overall/Administer permission.	4.8	More Details
CVE-2022-23321	A persistent cross-site scripting (XSS) vulnerability exists on two input fields within the administrative panel when editing users in the XMPie UStore application on version 12.3.7244.0.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44969	Taocms v3.0.2 was discovered to contain a cross-site scripting (XSS) vulnerability via the Management Column component.	4.8	More Details
CVE-2021-25050	The Remove Footer Credit WordPress plugin before 1.0.11 does properly sanitise its settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.	4.8	More Details
CVE-2021-24904	The Mortgage Calculators WP WordPress plugin before 1.56 does not implement any sanitisation on the color setting of the background of a calculator, which could allow high privilege users to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-22567	Select Dell Client Commercial and Consumer platforms are vulnerable to an insufficient verification of data authenticity vulnerability. An authenticated malicious user may exploit this vulnerability in order to install modified BIOS firmware.	4.7	More Details
CVE-2022-0019	An insufficiently protected credentials vulnerability exists in the Palo Alto Networks GlobalProtect app on Linux that exposes the hashed credentials of GlobalProtect users that saved their password during previous GlobalProtect app sessions to other local users on the system. The exposed credentials enable a local attacker to authenticate to the GlobalProtect portal or gateway as the target user without knowing of the target user's plaintext password. This issue impacts: GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.10 on Linux. GlobalProtect app 5.2 versions earlier than and including GlobalProtect app 5.2.7 on Linux. GlobalProtect app 5.3 versions earlier than GlobalProtect app 5.3.2 on Linux. This issue does not affect the GlobalProtect app on other platforms.	4.7	More Details
CVE-2021-40015	There is a race condition vulnerability in the binder driver subsystem in the kernel.Successful exploitation of this vulnerability may affect kernel stability.	4.7	More Details
CVE-2022-22780	The Zoom Client for Meetings chat functionality was susceptible to Zip bombing attacks in the following product versions: Android before version 5.8.6, iOS before version 5.9.0, Linux before version 5.8.6, macOS before version 5.7.3, and Windows before version 5.6.3. This could lead to availability issues on the client host by exhausting system resources.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23618	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions there is no protection against URL redirection to untrusted sites, in particular some well known parameters (xredirect) can be used to perform url redirections. This problem has been patched in XWiki 12.10.7 and XWiki 13.3RC1. Users are advised to update. There are no known workarounds for this issue.	4.7	More Details
CVE-2021-33107	Insufficiently protected credentials in USB provisioning for Intel(R) AMT SDK before version 16.0.3, Intel(R) SCS before version 12.2 and Intel(R) MEBx before versions 11.0.0.0012, 12.0.0.0011, 14.0.0.0004 and 15.0.0.0004 may allow an unauthenticated user to potentially enable information disclosure via physical access.	4.6	More Details
CVE-2021-40837	A vulnerability affecting F-Secure antivirus engine before Capricorn update 2022-02-01_01 was discovered whereby decompression of ACE file causes the scanner service to stop. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine.	4.6	More Details
CVE-2022-20033	In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973.	4.4	More Details
CVE-2021-0176	Improper input validation in firmware for some Intel(R) PROSet/Wireless Wi-Fi in multiple operating systems and some Killer(TM) Wi-Fi in Windows 10 and 11 may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details
CVE-2022-23426	A vulnerability using PendingIntent in DeX Home and DeX for PC prior to SMR Feb-2022 Release 1 allows attackers to access files with system privilege.	4.4	More Details
CVE-2021-0092	Improper access control in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable a denial of service via local access.	4.4	More Details
CVE-2021-0093	Incorrect default permissions in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable a denial of service via local access.	4.4	More Details
CVE-2021-0147	Improper locking in the Power Management Controller (PMC) for some Intel Chipset firmware before versions pmc_fw_lbg_c1-21ww02a and pmc_fw_lbg_b0-21ww02a may allow a privileged user to potentially enable denial of service via local access.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23434	A vulnerability using PendingIntent in Bixby Vision prior to versions 3.7.60.8 in Android S(12), 3.7.50.6 in Andorid R(11) and below allows attackers to execute privileged action by hijacking and modifying the intent.	4.4	More Details
CVE-2022-20029	In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150.	4.4	More Details
CVE-2021-44111	A Directory Traversal vulnerability exists in S-Cart 6.7 via download in sc-admin/backup.	4.4	More Details
CVE-2022-24925	Improper input validation vulnerability in SettingsProvider prior to Android S(12) allows privileged attackers to trigger a permanent denial of service attack on a victim's devices.	4.4	More Details
CVE-2022-20630	A vulnerability in the audit log of Cisco DNA Center could allow an authenticated, local attacker to view sensitive information in clear text. This vulnerability is due to the unsecured logging of sensitive information on an affected system. An attacker with administrative privileges could exploit this vulnerability by accessing the audit logs through the CLI. A successful exploit could allow the attacker to retrieve sensitive information that includes user credentials.	4.4	More Details
CVE-2022-20035	In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675.	4.4	More Details
CVE-2022-25188	Jenkins Fortify Plugin 20.2.34 and earlier does not sanitize the appName and appVersion parameters of its Pipeline steps, allowing attackers with Item/Configure permission to write or overwrite .xml files on the Jenkins controller file system with content not controllable by the attacker.	4.3	More Details
CVE-2022-25190	A missing permission check in Jenkins Conjur Secrets Plugin 1.0.11 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2022-24694	In Mahara 20.10 before 20.10.4, 21.04 before 21.04.3, and 21.10 before 21.10.1, the names of folders in the Files area can be seen by a person not owning the folders. (Only folder names are affected. Neither file names nor file contents are affected.)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45346	A Memory Leak vulnerability exists in SQLite Project SQLite3 3.35.1 and 3.37.0 via maliciously crafted SQL Queries (made via editing the Database File), it is possible to query a record, and leak subsequent bytes of memory that extend beyond the record, which could let a malicious user obtain sensitive information. NOTE: The developer disputes this as a vulnerability stating that If you give SQLite a corrupted database file and submit a query against the database, it might read parts of the database that you did not intend or expect.	4.3	More Details
CVE-2022-25180	Jenkins Pipeline: Groovy Plugin 2648.va9433432b33c and earlier includes password parameters from the original build in replayed builds, allowing attackers with Run/Replay permission to obtain the values of password parameters passed to previous builds of a Pipeline.	4.3	More Details
CVE-2022-25195	A missing permission check in Jenkins autonomiq Plugin 1.15 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials.	4.3	More Details
CVE-2022-21968	Microsoft SharePoint Server Security Feature Bypass Vulnerability	4.3	More Details
CVE-2021-39943	An authorization logic error in the External Status Check API in GitLab EE affecting all versions starting from 14.1 before 14.3.6, all versions starting from 14.4 before 14.4.4, all versions starting from 14.5 before 14.5.2, allowed a user to update the status of the check via an API call	4.3	More Details
CVE-2022-0118	Inappropriate implementation in WebShare in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially hide the contents of the Omnibox (URL bar) via a crafted HTML page.	4.3	More Details
CVE-2022-20680	A vulnerability in the web-based management interface of Cisco Prime Service Catalog could allow an authenticated, remote attacker to access sensitive information on an affected device. This vulnerability is due to improper enforcement of Administrator privilege levels for low-value sensitive data. An attacker with read-only Administrator access to the web-based management interface could exploit this vulnerability by sending a malicious HTTP request to the page that contains the sensitive data. A successful exploit could allow the attacker to collect sensitive information about users of the system and orders that have been placed using the application.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43953	Affected versions of Atlassian Jira Server and Data Center allow unauthenticated remote attackers to toggle the Thread Contention and CPU monitoring settings via a Cross-Site Request Forgery (CSRF) vulnerability in the /secure/admin/ViewInstrumentation.jspa endpoint. The affected versions are before version 8.13.16, and from version 8.14.0 before 8.20.5.	4.3	More Details
CVE-2021-43952	Affected versions of Atlassian Jira Server and Data Center allow unauthenticated remote attackers to restore the default configuration of fields via a Cross-Site Request Forgery (CSRF) vulnerability in the /secure/admin/RestoreDefaults.jspa endpoint. The affected versions are before version 8.21.0.	4.3	More Details
CVE-2022-0596	Improper Validation of Specified Quantity in Input in Packagist microweber/microweber prior to 1.2.11.	4.3	More Details
CVE-2021-43948	Affected versions of Atlassian Jira Service Management Server and Data Center allow authenticated remote attackers to view the names of private objects via an Improper Authorization vulnerability in the "Move objects" feature. The affected versions are before version 4.21.0.	4.3	More Details
CVE-2021-43950	Affected versions of Atlassian Jira Service Management Server and Data Center allow authenticated remote attackers to view import source configuration information via a Broken Access Control vulnerability in the Insight Import Source feature. The affected versions are before version 4.21.0.	4.3	More Details
CVE-2022-0110	Incorrect security UI in Autofill in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	4.3	More Details
CVE-2022-0112	Incorrect security UI in Browser UI in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to display missing URL or incorrect URL via a crafted URL.	4.3	More Details
CVE-2021-25110	The Futurio Extra WordPress plugin before 1.6.3 allows any logged in user, such as subscriber, to extract any other user's email address.	4.3	More Details
CVE-2022-23433	Improper access control vulnerability in Reminder prior to versions 12.3.01.3000 in Android S(12), 12.2.05.6000 in Android R(11) and 11.6.08.6000 in Andoid Q(10) allows attackers to register reminders or execute exporeted activities remotely.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0116	Inappropriate implementation in Compositing in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	4.3	More Details
CVE-2022-0532	An incorrect sysctls validation vulnerability was found in CRI-O 1.18 and earlier. The sysctls from the list of "safe" sysctls specified for the cluster will be applied to the host if an attacker is able to create a pod with a hostIPC and hostNetwork kernel namespace.	4.2	More Details
CVE-2022-24927	Improper privilege management vulnerability in Samsung Video Player prior to version 7.3.15.30 allows attackers to execute video files without permission.	4.2	More Details
CVE-2022-20032	In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822.	4.1	More Details
CVE-2022-23996	Unprotected component vulnerability in StTheaterModeReceiver in Wear OS 3.0 prior to Firmware update Feb-2022 Release allows untrusted applications to enable bedtime mode without a proper permission.	4.0	More Details
CVE-2022-24002	Improper Authorization vulnerability in Link Sharing prior to version 12.4.00.3 allows attackers to open protected activity via PreconditionActivity.	4.0	More Details
CVE-2022-23997	Unprotected component vulnerability in StTheaterModeDurationAlarmReceiver in Wear OS 3.0 prior to Firmware update Feb-2022 Release allows untrusted applications to disable theater mode without a proper permission.	4.0	More Details
CVE-2022-24003	Exposure of Sensitive Information vulnerability in Bixby Vision prior to version 3.7.50.6 allows attackers to access internal data of Bixby Vision via unprotected intent.	4.0	More Details
CVE-2022-24923	Improper access control vulnerability in Samsung SearchWidget prior to versions 2.3.00.6 in China models allows untrusted applications to load arbitrary URL and local files in webview.	4.0	More Details
CVE-2022-23995	Unprotected component vulnerability in StBedtimeModeAlarmReceiver in Wear OS 3.0 prior to Firmware update Feb-2022 Release allows untrusted applications to change bedtime mode without a proper permission.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23427	PendingIntent hijacking vulnerability in KnoxPrivacyNoticeReceiver prior to SMR Feb-2022 Release 1 allows local attackers to access media files without permission via implicit Intent.	3.9	More Details
CVE-2022-24000	PendingIntent hijacking vulnerability in DataUsageReminderReceiver prior to SMR Feb-2022 Release 1 allows local attackers to access media files without permission in KnoxPrivacyNoticeReceiver via implicit Intent.	3.9	More Details
CVE-2022-23999	PendingIntent hijacking vulnerability in CpaReceiver prior to SMR Feb-2022 Release 1 allows local attackers to access media files without permission in KnoxPrivacyNoticeReceiver via implicit Intent.	3.9	More Details
CVE-2022-24001	Information disclosure vulnerability in Edge Panel prior to Android S(12) allows physical attackers to access screenshot in clipboard via Edge Panel.	3.8	More Details
CVE-2022-22779	The Keybase Clients for macOS and Windows before version 5.9.0 fails to properly remove exploded messages initiated by a user. This can occur if the receiving user switches to a non-chat feature and places the host in a sleep state before the sending user explodes the messages. This could lead to disclosure of sensitive information which was meant to be deleted from a user’s filesystem.	3.7	More Details
CVE-2021-25014	The Ibtana WordPress plugin before 1.1.4.9 does not have authorisation and CSRF checks in the ive_save_general_settings AJAX action, allowing any authenticated users, such as subscriber to call it and change the plugin's settings which could lead to Stored Cross-Site Scripting issue.	3.5	More Details
CVE-2021-4035	A stored cross site scripting have been identified at the comments in the report creation due to an obsolete version of tinymce editor. In order to exploit this vulnerability, the attackers needs an account with enough privileges to view and edit reports.	3.5	More Details
CVE-2022-0021	An information exposure through log file vulnerability exists in the Palo Alto Networks GlobalProtect app on Windows that logs the cleartext credentials of the connecting GlobalProtect user when authenticating using Connect Before Logon feature. This issue impacts GlobalProtect App 5.2 versions earlier than 5.2.9 on Windows. This issue does not affect the GlobalProtect app on other platforms.	3.3	More Details
CVE-2022-23994	An Improper access control vulnerability in StBedtimeModeReceiver in Wear OS 3.0 prior to Firmware update Feb-2022 Release allows untrusted applications to change bedtime mode without a proper permission.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25109	The Futurio Extra WordPress plugin before 1.6.3 is affected by a SQL Injection vulnerability that could be used by high privilege users to extract data from the database as well as used to perform Cross-Site Scripting (XSS) against logged in admins by making send open a malicious link.	2.7	More Details
CVE-2021-25939	In ArangoDB, versions v3.7.0 through v3.9.0-alpha.1 have a feature which allows downloading a Foxx service from a publicly available URL. This feature does not enforce proper filtering of requests performed internally, which can be abused by a highly-privileged attacker to perform blind SSRF and send internal requests to localhost.	2.7	More Details
CVE-2022-0536	Improper Removal of Sensitive Information Before Storage or Transfer in NPM follow-redirects prior to 1.14.8.	2.6	More Details
CVE-2022-24924	An improper access control in LiveWallpaperService prior to versions 3.0.9.0 allows to create a specific named system directory without a proper permission.	2.2	More Details
CVE-2021-20011	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20015	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-40696	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-2021-37857	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-37856	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37855	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-37854	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-37853	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20002	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20010	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20003	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20004	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20005	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20006	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20007	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20008	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20014	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20013	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20012	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-20009	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details
CVE-2021-37858	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2021. Notes: none	N/A	More Details