SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 17 August 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-36010	This library allows strings to be parsed as functions and stored as a specialized component, [`JsonFunctionValue`](https://github.com/oxyno-zeta/react-editable-json-tree/blob/09a0ca97835b0834ad054563e2fddc6f22bc5d8c/src/components/JsonFunctionValue.js). To do this, Javascript's [`eval`](https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/eval) function is used to execute strings that begin with "function" as Javascript. This unfortunately could allow arbitrary code to be executed if it exists as a value within the JSON structure being displayed. Given that this component may often be used to display data from arbitrary, untrusted sources, this is extremely dangerous. One important note is that users who have defined a custom [`onSubmitValueParser`](https://github.com/oxyno-zeta/react-editable-json-tree/tree/09a0ca97835b0834ad054563e2fddc6f22bc5d8c#onsubmitvalueparser) callback prop on the [`JsonTree`](https://github.com/oxyno-zeta/react-editable-json-tree/blob/09a0ca97835b0834ad054563e2fddc6f22bc5d8c/src/JsonTree.js) component should be ***unaffected***. This vulnerability exists in the default `onSubmitValueParser` prop which calls [`parse`](https://github.com/oxyno-zeta/react-editable-json-tree/blob/master/src/utils/parse.js#L30). Prop is added to `JsonTree` called `allowFunctionEvaluation`. This prop will be set to `true` in v2.2.2, which allows upgrade without losing backwards-compatibility. In v2.2.2, we switched from using `eval` to using [`Function`](https://developer.mozilla.org/en-US/docs/Web/JavaScript/Reference/Global_Objects/Function) to construct anonymous functions. This is better than `eval` for the following reasons: - Arbitrary code should not be able to execute immediately, since the `Function` constructor explicitly *only creates* anonymous functions - Functions are created without local closures, so they only have access to the global scope If you use: - **Version `<2.2.2`**, you must upgrade as soon as possible. - **Version `^2.2.2`**, you must explicitly set `JsonTree`'s `allowFunctionEvaluation` prop to `false` to fully mitigate this vulnerability. - **Version `>=3.0.0`**, `allowFunctionEvaluation` is already set to `false` by default, so no further steps are necessary.	10.0	More Details
CVE-2022-2634	An attacker may be able to execute malicious actions due to the lack of device access protections and device permissions when using the web application. This could lead to uploading python files which can be later executed.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2661	Sequi PortBloque S has an improper authorization vulnerability, which may allow a low-privileged user to perform administrative functions using specifically crafted requests.	9.9	More Details
CVE-2022-38130	The com.keysight.tentacle.config.ResourceManager.smsRestoreDatabaseZip() method is used to restore the HSQLDB database used in SMS. It takes the path of the zipped database file as the single parameter. An unauthenticated, remote attacker can specify an UNC path for the database file (i.e., \\<attacker-host>\sms\<attacker-db.zip>), effectively controlling the content of the database to be restored.	9.8	More Details
CVE-2022-20381	Product: AndroidVersions: Android kernelAndroid ID: A-188935887References: N/A	9.8	More Details
CVE-2022-20403	Product: AndroidVersions: Android kernelAndroid ID: A-207975764References: N/A	9.8	More Details
CVE-2022-20402	Product: AndroidVersions: Android kernelAndroid ID: A-218701042References: N/A	9.8	More Details
CVE-2022-20400	In cd_CodeMsg of cd_codec.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-225178325References: N/A	9.8	More Details
CVE-2022-20384	Product: AndroidVersions: Android kernelAndroid ID: A-211727306References: N/A	9.8	More Details
CVE-2022-20365	Product: AndroidVersions: Android kernelAndroid ID: A-229632566References: N/A	9.8	More Details
CVE-2022-20378	Product: AndroidVersions: Android kernelAndroid ID: A-234657153References: N/A	9.8	More Details
CVE-2022-36272	Mingsoft MCMS 5.2.8 was discovered to contain a SQL injection vulnerability in /mdiy/page/verify URI via fieldName parameter.	9.8	More Details
CVE-2022-20237	In BuildDevIDResponse of miscdatabuilder.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-229621649References: N/A	9.8	More Details
CVE-2022-36273	Tenda AC9 V15.03.2.21_cn is vulnerable to command injection via goform/SetSysTimeCfg.	9.8	More Details
CVE-2022-38129	A path traversal vulnerability exists in the com.keysight.tentacle.licensing.LicenseManager.addLicenseFile() method in the Keysight Sensor Management Server (SMS). This allows an unauthenticated remote attacker to upload arbitrary files to the SMS host.	9.8	More Details
CVE-2022-37003	The AOD module has a vulnerability in permission assignment. Successful exploitation of this vulnerability may cause permission escalation and unauthorized access to files.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20405	Product: AndroidVersions: Android kernelAndroid ID: A-216363416References: N/A	9.8	More Details
CVE-2022-35559	A stack overflow vulnerability exists in /goform/setAutoPing in Tenda W6 V1.0.0.9(4122), which allows an attacker to construct ping1 parameters and ping2 parameters for a stack overflow attack. An attacker can use this vulnerability to execute arbitrary code execution.	9.8	More Details
CVE-2022-35555	A command injection vulnerability exists in /goform/exeCommand in Tenda W6 V1.0.0.9(4122), which allows attackers to construct cmdinput parameters for arbitrary command execution.	9.8	More Details
CVE-2022-36750	Clinic's Patient Management System v1.0 is vulnerable to SQL injection via /pms/update_user.php?id=.	9.8	More Details
CVE-2022-37042	Zimbra Collaboration Suite (ZCS) 8.8.15 and 9.0 has mboximport functionality that receives a ZIP archive and extracts files from it. By bypassing authentication (i.e., not having an authtoken), an attacker can upload arbitrary files to the system, leading to directory traversal and remote code execution. NOTE: this issue exists because of an incomplete fix for CVE-2022-27925.	9.8	More Details
CVE-2022-2587	Out of bounds write in Chrome OS Audio Server in Google Chrome on Chrome OS prior to 102.0.5005.125 allowed a remote attacker to potentially exploit heap corruption via crafted audio metadata.	9.8	More Details
CVE-2022-30264	The Emerson ROC and FloBoss RTU product lines through 2022-05-02 perform insecure filesystem operations. They utilize the ROC protocol (4000/TCP, 5000/TCP) for communications between a master terminal and RTUs. Opcode 203 of this protocol allows a master terminal to transfer files to and from the flash filesystem and carrying out arbitrary file and directory read, write, and delete operations.	9.8	More Details
CVE-2022-2180	The GREYD.SUITE WordPress theme does not properly validate uploaded custom font packages, and does not perform any authorization or csrf checks, allowing an unauthenticated attacker to upload arbitrary files including php source files, leading to possible remote code execution (RCE).	9.8	More Details
CVE-2022-2314	The VR Calendar WordPress plugin through 2.3.2 lets any user execute arbitrary PHP functions on the site.	9.8	More Details
CVE-2022-2818	Improper Removal of Sensitive Information Before Storage or Transfer in GitHub repository cockpit-hq/cockpit prior to 2.2.2.	9.8	More Details
CVE-2022-38221	A buffer overflow in the FTcpListener thread in The Isle Evrima (the dedicated server on Windows and Linux) 0.9.88.07 before 2022-08-12 allows a remote attacker to crash any server with an accessible RCON port, or possibly execute arbitrary code.	9.8	More Details
CVE-2022-34294	totd 1.5.3 uses a fixed UDP source port in upstream queries sent to DNS resolvers. This allows DNS cache poisoning because there is not enough entropy to prevent traffic injection attacks.	9.8	More Details
CVE-2022-36262	An issue was discovered in taocms 3.0.2. in the website settings that allows arbitrary php code to be injected by modifying config.php.	9.8	More Details
CVE-2022-36523	D-Link Go-RT-AC750 GORTAC750_revA_v101b03 & GO-RT-AC750_revB_FWv200b02 is vulnerable to command injection via /htdocs/upnpinc/gena.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36525	D-Link Go-RT-AC750 GORTAC750_revA_v101b03 & GO-RT-AC750_revB_FWv200b02 is vulnerable to Buffer Overflow via authenticationcgi_main.	9.8	More Details
CVE-2022-37002	The SystemUI module has a privilege escalation vulnerability. Successful exploitation of this vulnerability can cause malicious applications to pop up windows or run in the background.	9.8	More Details
CVE-2022-36270	Clinic's Patient Management System v1.0 has arbitrary code execution via url: ip/pms/users.php.	9.8	More Details
CVE-2022-36344	An unquoted search path vulnerability exists in 'JustSystems JUST Online Update for J-License' bundled with multiple products for corporate users as in Ichitaro through Pro5 and others. Since the affected product starts another program with an unquoted file path, a malicious file may be executed with the privilege of the Windows service if it is placed in a certain path. Affected products are bundled with the following product series: Office and Office Integrated Software, ATOK, Hanako, JUST PDF, Shuriken, Homepage Builder, JUST School, JUST Smile Class, JUST Smile, JUST Frontier, JUST Jump, and Tri-De DetaProtect.	9.8	More Details
CVE-2022-35518	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 nas.cgi has no filtering on parameters: User1Passwd and User1, which leads to command injection in page /nas_disk.shtml.	9.8	More Details
CVE-2022-2242	The KUKA SystemSoftware V/KSS in versions prior to 8.6.5 is prone to improper access control as an unauthorized attacker can directly read and write robot configurations when access control is not available or not enabled (default).	9.8	More Details
CVE-2022-34660	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter consist of a functionality that is vulnerable to command injection. This could potentially allow an attacker to perform remote code execution.	9.8	More Details
CVE-2021-39085	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.5, 6.1.0.0 through 6.1.0.4, and 6.1.1.0 through 6.1.1.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 215888.	9.8	More Details
CVE-2022-35280	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 230634.	9.8	More Details
CVE-2022-36242	Clinic's Patient Management System v1.0 is vulnerable to SQL Injection via /pms/update_medicine.php?id=.	9.8	More Details
CVE-2022-20239	remap_pfn_range' here may map out of size kernel memory (for example, may map the kernel area), and because the 'vma->vm_page_prot' can also be controlled by userspace, so userspace may map the kernel area to be writable, which is easy to be exploitedProduct: AndroidVersions: Android SoCAndroid ID: A-233972091	9.8	More Details
CVE-2022-20361	In btif_dm_auth_cmpl_evt of btif_dm.cc, there is a possible vulnerability in Cross-Transport Key Derivation due to Weakness in Bluetooth Standard. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-231161832	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2457	A flaw was found in Red Hat Process Automation Manager 7 where an attacker can benefit from a brute force attack against Administration Console as the application does not limit the number of unsuccessful login attempts.	9.8	More Details
CVE-2022-32429	An authentication-bypass issue in the component http://MYDEVICEIP/cgi-bin-sdb/ExportSettings.sh of Mega System Technologies Inc MSNSwitch MNT.2408 allows unauthenticated attackers to arbitrarily configure settings within the application, leading to remote code execution.	9.8	More Details
CVE-2022-36599	Mingsoft MCMS 5.2.8 was discovered to contain a SQL injection vulnerability in /mdiy/model/delete URI via models Lists.	9.8	More Details
CVE-2022-35426	UCMS 1.6 is vulnerable to arbitrary file upload via ucms/sadmin/file PHP file.	9.8	More Details
CVE-2022-35491	TOTOLINK A3002RU V3.0.0-B20220304.1804 has a hardcoded password for root in /etc/shadow.sample.	9.8	More Details
CVE-2022-35519	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter add_mac, which leads to command injection in page /cli_black_list.shtml.	9.8	More Details
CVE-2022-35538	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: delete_list, delete_al_mac, b_delete_list and b_delete_al_mac, which leads to command injection in page /wifi_mesh.shtml.	9.8	More Details
CVE-2022-35520	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 api.cgi has no filtering on parameter ufconf, and this is a hidden parameter which doesn't appear in POST body, but exist in cgi binary. This leads to command injection in page /ledonoff.shtml.	9.8	More Details
CVE-2022-35521	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameters: remoteManagementEnabled, blockPortScanEnabled, pingFrmWANFilterEnabled and blockSynFloodEnabled, which leads to command injection in page /man_security.shtml.	9.8	More Details
CVE-2022-35522	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: ppp_username, ppp_passwd, rwan_gateway, rwan_mask and rwan_ip, which leads to command injection in page /wan.shtml.	9.8	More Details
CVE-2022-35523	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 firewall.cgi has no filtering on parameter del_mac and parameter flag, which leads to command injection in page /cli_black_list.shtml.	9.8	More Details
CVE-2022-35524	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: wlan_signal, web_pskValue, sel_EncrypTyp, sel_Automode, wlan_bssid, wlan_ssid and wlan_channel, which leads to command injection in page /wizard_rep.shtml.	9.8	More Details
CVE-2022-35525	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameter led_switch, which leads to command injection in page /ledonoff.shtml.	9.8	More Details
CVE-2022-35526	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 login.cgi has no filtering on parameter key, which leads to command injection in page /login.shtml.	9.8	More Details
CVE-2022-35533	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: cli_list and cli_num, which leads to command injection in page /qos.shtml.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35534	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter hiddenSSID32g and SSID2G2, which leads to command injection in page /wifi_multi_ssid.shtml.	9.8	More Details
CVE-2022-35535	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameter macAddr, which leads to command injection in page /wifi_mesh.shtml.	9.8	More Details
CVE-2022-35536	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 qos.cgi has no filtering on parameters: qos_bandwith and qos_dat, which leads to command injection in page /qos.shtml.	9.8	More Details
CVE-2022-35537	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 wireless.cgi has no filtering on parameters: mac_5g and Newname, which leads to command injection in page /wifi_mesh.shtml.	9.8	More Details
CVE-2020-21642	Directory Traversal vulnerability ZDBQAREFSUBDIR parameter in /zropusermgmt API in Zoho ManageEngine Analytics Plus before 4350 allows remote attackers to run arbitrary code.	9.8	More Details
CVE-2022-2662	Sequi PortBloque S has a improper authentication issues which may allow an attacker to bypass the authentication process and gain user-level access to the device.	9.6	More Details
CVE-2022-28755	The Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.11.0 are susceptible to a URL parsing vulnerability. If a malicious Zoom meeting URL is opened, the malicious link may direct the user to connect to an arbitrary network address, leading to additional attacks including the potential for remote code execution through launching executables from arbitrary paths.	9.6	More Details
CVE-2022-35942	Improper input validation on the `contains` LoopBack filter may allow for arbitrary SQL injection. When the extended filter property `contains` is permitted to be interpreted by the Postgres connector, it is possible to inject arbitrary SQL which may affect the confidentiality and integrity of data stored on the connected database. A patch was released in version 5.5.1. This affects users who does any of the following: - Connect to the database via the DataSource with `allowExtendedProperties: true` setting OR - Uses the connector's CRUD methods directly OR - Uses the connector's other methods to interpret the LoopBack filter. Users who are unable to upgrade should do the following if applicable: - Remove `allowExtendedProperties: true` DataSource setting - Add `allowExtendedProperties: false` DataSource setting - When passing directly to the connector functions, manually sanitize the user input for the `contains` LoopBack filter beforehand.	9.3	More Details
CVE-2022-36308	Airspan AirVelocity 1500 web management UI displays SNMP credentials in plaintext on software versions older than 15.18.00.2511, and stores SNMPv3 credentials unhashed on the filesystem, enabling anyone with web access to use these credentials to manipulate the eNodeB over SNMP. This issue may affect other AirVelocity and AirSpeed models.	9.1	More Details
CVE-2022-35293	Due to insecure session management, SAP Enable Now allows an unauthenticated attacker to gain access to user's account. On successful exploitation, an attacker can view or modify user data causing limited impact on confidentiality and integrity of the application.	9.1	More Details
CVE-2021-33643	An attacker who submits a crafted tar file with size in header struct being 0 may be able to trigger an calling of malloc(0) for a variable gnu_longlink, causing an out-of-bounds read.	9.1	More Details
CVE-2022-36323	Affected devices do not properly sanitize an input field. This could allow an authenticated remote attacker with administrative privileges to inject code or spawn a system root shell.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20827	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	9.0	More Details
CVE-2022-20842	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	9.0	More Details
CVE-2022-20841	Multiple vulnerabilities in Cisco Small Business RV160, RV260, RV340, and RV345 Series Routers could allow an unauthenticated, remote attacker to execute arbitrary code or cause a denial of service (DoS) condition on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-14321	In Moodle before 3.9.1, 3.8.4, 3.7.7 and 3.5.13, teachers of a course were able to assign themselves the manager role within that course.	8.8	More Details
CVE-2022-37401	Apache OpenOffice supports the storage of passwords for web connections in the user's configuration database. The stored passwords are encrypted with a single master key provided by the user. A flaw in OpenOffice existed where master key was poorly encoded resulting in weakening its entropy from 128 to 43 bits making the stored passwords vulnerable to a brute force attack if an attacker has access to the users stored config. This issue affects: Apache OpenOffice versions prior to 4.1.13. Reference: CVE-2022-26307 - LibreOffice	8.8	More Details
CVE-2022-2620	Use after free in WebUI in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.	8.8	More Details
CVE-2022-2621	Use after free in Extensions in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interactions.	8.8	More Details
CVE-2022-2623	Use after free in Offline in Google Chrome on Android prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.	8.8	More Details
CVE-2022-20345	In l2cble_process_sig_cmd of l2c_ble.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-230494481	8.8	More Details
CVE-2022-2624	Heap buffer overflow in PDF in Google Chrome prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted PDF file.	8.8	More Details
CVE-2022-35517	WAVLINK WN572HP3, WN533A8, WN530H4, WN535G3, WN531P3 adm.cgi has no filtering on parameters: web_pskValue, wl_Method, wlan_ssid, EncrypType, rwan_ip, rwan_mask, rwan_gateway, ppp_username, ppp_passwd and ppp_setver, which leads to command injection in page /wizard_router_mesh.shtml.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28756	The Zoom Client for Meetings for macOS (Standard and for IT Admin) starting with version 5.7.3 and before 5.11.5 contains a vulnerability in the auto update process. A local low-privileged user could exploit this vulnerability to escalate their privileges to root.	8.8	More Details
CVE-2022-38362	Apache Airflow Docker's Provider prior to 3.0.0 shipped with an example DAG that was vulnerable to (authenticated) remote code exploit of code on the Airflow worker host.	8.8	More Details
CVE-2022-2824	Authorization Bypass Through User-Controlled Key in GitHub repository openemr/openemr prior to 7.0.0.1.	8.8	More Details
CVE-2022-2381	The E Unlocked - Student Result WordPress plugin through 1.0.4 is lacking CSRF and validation when uploading the School logo, which could allow attackers to make a logged in admin upload arbitrary files, such as PHP via a CSRF attack	8.8	More Details
CVE-2022-35239	The image file management page of SolarView Compact SV-CPT-MC310 Ver.7.23 and earlier, and SV-CPT-MC310F Ver.7.23 and earlier contains an insufficient verification vulnerability when uploading files. If this vulnerability is exploited, arbitrary PHP code may be executed if a remote authenticated attacker uploads a specially crafted PHP file.	8.8	More Details
CVE-2022-31673	VMware vRealize Operations contains an information disclosure vulnerability. A low-privileged malicious actor with network access can create and leak hex dumps, leading to information disclosure. Successful exploitation can lead to a remote code execution.	8.8	More Details
CVE-2022-38357	Improper neutralization of special elements leaves the Eyes of Network Web application vulnerable to an iFrame injection attack, via the url parameter of /module/module_frame/index.php.	8.8	More Details
CVE-2022-38359	Cross-site request forgery attacks can be carried out against the Eyes of Network web application, due to an absence of adequate protections. An attacker can, for instance, delete the admin user by directing an authenticated user to the URL https://<target-address>/module/admin_user/index.php?DataTables_Table_0_length=10&user_selected%5B%5D=1&user_mgt_list=delete_user&action=submit by means of a crafted link.	8.8	More Details
CVE-2022-36312	Airspan AirVelocity 1500 software version 15.18.00.2511 lacks CSRF protections in the eNodeB's web management UI. This issue may affect other AirVelocity and AirSpeed models.	8.8	More Details
CVE-2022-36310	Airspan AirVelocity 1500 software prior to version 15.18.00.2511 had NET-SNMP-EXTEND-MIB enabled on its snmpd service, enabling an attacker with SNMP write abilities to execute commands as root on the eNodeB. This issue may affect other AirVelocity and AirSpeed models.	8.8	More Details
CVE-2022-37400	Apache OpenOffice supports the storage of passwords for web connections in the user's configuration database. The stored passwords are encrypted with a single master key provided by the user. A flaw in OpenOffice existed where the required initialization vector for encryption was always the same which weakens the security of the encryption making them vulnerable if an attacker has access to the user's configuration data. This issue affects: Apache OpenOffice versions prior to 4.1.13. Reference: CVE-2022-26306 - LibreOffice	8.8	More Details
CVE-2022-2617	Use after free in Extensions API in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interactions.	8.8	More Details
CVE-2022-34254	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could be abused by an attacker to inject malicious scripts into the vulnerable endpoint. A low privileged attacker could leverage this vulnerability to read local files and to perform Stored XSS. Exploitation of this issue does not require user interaction.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34255	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an Improper Access Control vulnerability that could result in Privilege escalation. An attacker with a low privilege account could leverage this vulnerability to perform an account takeover for a victim. Exploitation of this issue does not require user interaction.	8.8	More Details
CVE-2022-2604	Use after free in Safe Browsing in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-20254	In Wi-Fi, there is a permissions bypass. This could lead to local escalation of privilege from the guest user with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-223377547	8.8	More Details
CVE-2022-20283	In Bluetooth, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-233069336	8.8	More Details
CVE-2022-20347	In onAttach of ConnectedDeviceDashboardFragment.java, there is a possible permission bypass due to a confused deputy. This could lead to remote escalation of privilege in Bluetooth settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228450811	8.8	More Details
CVE-2022-20362	In Bluetooth, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-230756082	8.8	More Details
CVE-2022-38368	An issue was discovered in Aviatrix Gateway before 6.6.5712 and 6.7.x before 6.7.1376. Because Gateway API functions mishandle authentication, an authenticated VPN user can inject arbitrary commands.	8.8	More Details
CVE-2022-28631	A potential arbitrary code execution and a denial of service (DoS) vulnerability within an isolated process were discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Prior to 2.71. An unprivileged user could exploit this vulnerability in an adjacent network to potentially execute arbitrary code in an isolated process resulting in a complete loss of confidentiality, integrity, and availability within that process. In addition, an unprivileged user could exploit a denial of service (DoS) vulnerability in an isolated process resulting in a complete loss of availability within that process. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 5 (iLO 5).	8.8	More Details
CVE-2022-28632	A potential arbitrary code execution and a denial of service (DoS) vulnerability within an isolated process were discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Prior to 2.71. An unprivileged user could exploit this vulnerability in an adjacent network to potentially execute arbitrary code in an isolated process resulting in a complete loss of confidentiality, integrity, and availability within that process. In addition, an unprivileged user could exploit a denial of service (DoS) vulnerability in an isolated process resulting in a complete loss of availability within that process. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 5 (iLO 5).	8.8	More Details
CVE-2022-2603	Use after free in Omnibox in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2606	Use after free in Managed devices API in Google Chrome prior to 104.0.5112.79 allowed a remote attacker who convinced a user to enable a specific Enterprise policy to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-2607	Use after free in Tab Strip in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2608	Use after free in Overview Mode in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.	8.8	More Details
CVE-2022-37024	Zoho ManageEngine OpManager, OpManager Plus, OpManager MSP, Network Configuration Manager, NetFlow Analyzer, and OpUtils before 2022-07-29 through 2022-07-30 (125658, 126003, 126105, and 126120) allow authenticated users to make database changes that lead to remote code execution.	8.8	More Details
CVE-2022-35011	PNGDec commit 8abf6be was discovered to contain a global buffer overflow via inflate_fast at /src/inffast.c.	8.8	More Details
CVE-2022-2609	Use after free in Nearby Share in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.	8.8	More Details
CVE-2022-2613	Use after free in Input in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to enage in specific user interactions to potentially exploit heap corruption via specific UI interactions.	8.8	More Details
CVE-2022-2614	Use after free in Sign-In Flow in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	8.8	More Details
CVE-2022-36309	Airspan AirVelocity 1500 software versions prior to 15.18.00.2511 have a root command injection vulnerability in the ActiveBank parameter of the recoverySubmit.cgi script running on the eNodeB's web management UI. This issue may affect other AirVelocity and AirSpeed models.	8.8	More Details
CVE-2022-30576	The Web Console component of TIBCO Software Inc.'s TIBCO Data Science - Workbench, TIBCO Statistica, TIBCO Statistica - Estore Edition, and TIBCO Statistica Trial contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute Stored Cross Site Scripting (XSS) on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Data Science - Workbench: versions 14.0.0 and below, TIBCO Statistica: versions 14.0.0 and below, TIBCO Statistica - Estore Edition: versions 14.0.0 and below, and TIBCO Statistica Trial: versions 14.0.0 and below.	8.7	More Details
CVE-2022-0028	A PAN-OS URL filtering policy misconfiguration could allow a network-based attacker to conduct reflected and amplified TCP denial-of-service (RDoS) attacks. The DoS attack would appear to originate from a Palo Alto Networks PA-Series (hardware), VM-Series (virtual) and CN-Series (container) firewall against an attacker-specified target. To be misused by an external attacker, the firewall configuration must have a URL filtering profile with one or more blocked categories assigned to a source zone that has an external facing interface. This configuration is not typical for URL filtering and, if set, is likely unintended by the administrator. If exploited, this issue would not impact the confidentiality, integrity, or availability of our products. However, the resulting denial-of-service (DoS) attack may help obfuscate the identity of the attacker and implicate the firewall as the source of the attack. We have taken prompt action to address this issue in our PAN-OS software. All software updates for this issue are expected to be released no later than the week of August 15, 2022. This issue does not impact Panorama M-Series or Panorama virtual appliances. This issue has been resolved for all Cloud NGFW and Prisma Access customers and no additional action is required from them.	8.6	More Details
CVE-2022-29090	Dell Wyse Management Suite 3.6.1 and below contains a Sensitive Data Exposure vulnerability. A low privileged malicious user could potentially exploit this vulnerability in order to obtain credentials. The attacker may be able to use the exposed credentials to access the target device and perform unauthorized actions.	8.5	More Details
CVE-2022-28628	A local arbitrary code execution vulnerability was discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Prior to 2.71. An unprivileged user could locally exploit this vulnerability to execute arbitrary code resulting in a complete loss of confidentiality, integrity, and availability. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 5 (iLO 5).	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28627	A local arbitrary code execution vulnerability was discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Prior to 2.71. An unprivileged user could locally exploit this vulnerability to execute arbitrary code resulting in a complete loss of confidentiality, integrity, and availability. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 5 (iLO 5).	8.4	More Details
CVE-2022-37397	An issue was discovered in the YugabyteDB 2.6.1 when using LDAP-based authentication in YCQL with Microsoft's Active Directory. When anonymous or unauthenticated LDAP binding is enabled, it allows bypass of authentication with an empty password.	8.3	More Details
CVE-2021-22289	Improper Input Validation vulnerability in the project upload mechanism in B&R Automation Studio version >=4.0 may allow an unauthenticated network attacker to execute code.	8.3	More Details
CVE-2022-2458	XML external entity injection(XXE) is a vulnerability that allows an attacker to interfere with an application's processing of XML data. This attack occurs when XML input containing a reference to an external entity is processed by a weakly configured XML parser. The software processes an XML document that can contain XML entities with URIs that resolve to documents outside of the intended sphere of control, causing the product to embed incorrect documents into its output. Here, XML external entity injection lead to External Service interaction & Internal file read in Business Central and also Kie-Server APIs.	8.2	More Details
CVE-2022-32245	SAP BusinessObjects Business Intelligence Platform (Open Document) - versions 420, 430, allows an unauthenticated attacker to retrieve sensitive information plain text over the network. On successful exploitation, the attacker can view any data available for a business user and put load on the application by an automated attack. Thus, completely compromising confidentiality but causing a limited impact on the availability of the application.	8.2	More Details
CVE-2022-35624	In Nordic nRF5 SDK for Mesh 5.0, a heap overflow vulnerability can be triggered by sending a series of segmented packets with SegO > SegN	8.2	More Details
CVE-2022-35623	In Nordic nRF5 SDK for Mesh 5.0, a heap overflow vulnerability can be triggered by sending a series of segmented control packets and access packets with the same SeqAuth	8.2	More Details
CVE-2021-33644	An attacker who submits a crafted tar file with size in header struct being 0 may be able to trigger an calling of malloc(0) for a variable gnu_longname, causing an out-of-bounds read.	8.1	More Details
CVE-2022-35961	OpenZeppelin Contracts is a library for secure smart contract development. The functions `ECDSA.recover` and `ECDSA.tryRecover` are vulnerable to a kind of signature malleability due to accepting EIP-2098 compact signatures in addition to the traditional 65 byte signature format. This is only an issue for the functions that take a single `bytes` argument, and not the functions that take `r, v, s` or `r, vs` as separate arguments. The potentially affected contracts are those that implement signature reuse or replay protection by marking the signature itself as used rather than the signed message or a nonce included in it. A user may take a signature that has already been submitted, submit it again in a different form, and bypass this protection. The issue has been patched in 4.7.3.	7.9	More Details
CVE-2022-36006	Arvados is an open source platform for managing, processing, and sharing genomic and other large scientific and biomedical data. A remote code execution (RCE) vulnerability in the Arvados Workbench allows authenticated attackers to execute arbitrary code via specially crafted JSON payloads. This exists in all versions up to 2.4.1 and is fixed in 2.4.2. This vulnerability is specific to the Ruby on Rails Workbench application ("Workbench 1"). We do not believe any other Arvados components, including the TypesScript browser-based Workbench application ("Workbench 2") or API Server, are vulnerable to this attack. For versions of Arvados earlier than 2.4.2: remove the Ruby-based "Workbench 1" app ("apt-get remove arvados-workbench") from your installation as a workaround.	7.9	More Details
CVE-2022-2816	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.0212.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36143	SWFMill commit 53d7690 was discovered to contain a heap-buffer overflow via __interceptor_strlen.part at /sanitizer_common/sanitizer_common_interceptors.inc.	7.8	More Details
CVE-2022-20180	In several functions of mali_gralloc_reference.cpp, there is a possible arbitrary code execution due to a missing bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-212804042References: N/A	7.8	More Details
CVE-2022-38237	XPDF commit ffaf11c was discovered to contain a heap-buffer overflow via DCTStream::readScan() at /xpdf/Stream.cc.	7.8	More Details
CVE-2022-38236	XPDF commit ffaf11c was discovered to contain a global-buffer overflow via Lexer::getObj(Object*) at /xpdf/Lexer.cc.	7.8	More Details
CVE-2022-20286	In Connectivity, there is a possible bypass the restriction of starting activity from background due to a logic error in the code. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-230866011	7.8	More Details
CVE-2022-20292	In Settings, there is a possible way to bypass factory reset protections due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-202975040	7.8	More Details
CVE-2022-20297	In Settings, there is a possible way to bypass factory reset protections due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-201561699	7.8	More Details
CVE-2022-20319	In DreamServices, there is a possible way to launch arbitrary protected activities 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-13Android ID: A-189574230	7.8	More Details
CVE-2022-20325	In Media, there is a possible code execution 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.Product: AndroidVersions: Android-13Android ID: A-186473060	7.8	More Details
CVE-2022-20329	In Wifi, there is a possible way to enable Wifi without permissions 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.Product: AndroidVersions: Android-13Android ID: A-183410556	7.8	More Details
CVE-2022-20331	In the Framework, there is a possible way to enable a work profile without user consent 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-13Android ID: A-181785557	7.8	More Details
CVE-2022-38231	XPDF commit ffaf11c was discovered to contain a heap-buffer overflow via DCTStream::getChar() at /xpdf/Stream.cc.	7.8	More Details
CVE-2022-38229	XPDF commit ffaf11c was discovered to contain a heap-buffer overflow via DCTStream::readHuffSym(DCTHuffTable*) at /xpdf/Stream.cc.	7.8	More Details
CVE-2022-25973	All versions of package mc-kill-port are vulnerable to Arbitrary Command Execution via the kill function, due to missing sanitization of the port argument.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28629	A local arbitrary code execution vulnerability was discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Prior to 2.71. A low privileged user could locally exploit this vulnerability to execute arbitrary code resulting in a complete loss of confidentiality, integrity, and availability. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 5 (iLO 5).	7.8	More Details
CVE-2022-38228	XPDF commit ffaf11c was discovered to contain a heap-buffer overflow via DCTStream::transformDataUnit at /xpdf/Stream.cc.	7.8	More Details
CVE-2022-20792	A vulnerability in the regex module used by the signature database load module of Clam AntiVirus (ClamAV) versions 0.104.0 through 0.104.2 and LTS version 0.103.5 and prior versions could allow an authenticated, local attacker to crash ClamAV at database load time, and possibly gain code execution. The vulnerability is due to improper bounds checking that may result in a multi-byte heap buffer overwflow write. An attacker could exploit this vulnerability by placing a crafted CDB ClamAV signature database file in the ClamAV database directory. An exploit could allow the attacker to run code as the clamav user.	7.8	More Details
CVE-2021-29117	A use-after-free vulnerability when parsing a specially crafted file in Esri ArcReader 10.8.1 (and earlier) allows an unauthenticated attacker to achieve arbitrary code execution in the context of the current user.	7.8	More Details
CVE-2022-38227	XPDF commit ffaf11c was discovered to contain a stack overflow via __asan_memcpy at asan_interceptors_memintrinsics.cpp.	7.8	More Details
CVE-2022-37781	fdkaac v1.0.3 was discovered to contain a heap buffer overflow via __interceptor_memcpy.part.46 at /sanitizer_common/sanitizer_common_interceptors.inc.	7.8	More Details
CVE-2022-20282	In AppWidget, there is a possible way to start an activity from the background due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-204083104	7.8	More Details
CVE-2022-20281	In Core, there is a possible way to start an activity from the background 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-13Android ID: A-204083967	7.8	More Details
CVE-2022-20274	In Keyguard, there is a missing permission check. This could lead to local escalation of privilege and prevention of screen timeout with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-206470146	7.8	More Details
CVE-2022-35674	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-34235	Adobe Premiere Elements version 2020v20 (and earlier) is affected by an Uncontrolled Search Path Element which could lead to Privilege Escalation. An attacker could leverage this vulnerability to obtain admin using an existing low-privileged user. Exploitation of this issue does not require user interaction.	7.8	More Details
CVE-2022-34260	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-34263	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35665	Adobe Acrobat Reader versions 22.001.20169 (and earlier), 20.005.30362 (and earlier) and 17.012.30249 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-35666	Adobe Acrobat Reader versions 22.001.20169 (and earlier), 20.005.30362 (and earlier) and 17.012.30249 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-35667	Adobe Acrobat Reader versions 22.001.20169 (and earlier), 20.005.30362 (and earlier) and 17.012.30249 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-35673	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-20368	Product: AndroidVersions: Android kernelAndroid ID: A-224546354References: Upstream kernel	7.8	More Details
CVE-2022-35675	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-20271	In PermissionController, there is a possible way to grant some permissions without user consent due to misleading or insufficient UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-207672635	7.8	More Details
CVE-2022-35676	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-35677	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-20250	In Messaging, there is a possible way to attach files to a message without proper access checks due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-226134095	7.8	More Details
CVE-2022-38238	XPDF commit ffaf11c was discovered to contain a heap-buffer overflow via DCTStream::lookChar() at /xpdf/Stream.cc.	7.8	More Details
CVE-2022-20248	In Settings, there is a possible way to connect to an open network bypassing DISALLOW_CONFIG_WIFI restriction due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-227619193	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20258	In Bluetooth, there is a possible way to bypass compiler exploit mitigations 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: AndroidVersions: Android-13Android ID: A-221893030	7.8	More Details
CVE-2022-20246	In WindowManager, there is a possible bypass of the restrictions for starting activities from the background due to an incorrect UID/permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-230493191	7.8	More Details
CVE-2022-20268	In RestrictionsManager, there is a possible way to send a broadcast that should be restricted to system apps due to a permissions bypass. This could lead to local escalation of privilege on an enterprise managed device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-210468836	7.8	More Details
CVE-2022-36144	SWFMill commit 53d7690 was discovered to contain a heap-buffer overflow via base64_encode.	7.8	More Details
CVE-2022-20383	In AllocateInternalBuffers of g3aa_buffer_allocator.cc, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-222408847References: N/A	7.8	More Details
CVE-2022-36142	SWFMill commit 53d7690 was discovered to contain a heap-buffer overflow via SWF::Reader::getU30().	7.8	More Details
CVE-2020-10728	A flaw was found in automationbroker/apb container in versions up to and including 2.0.4-1. This container grants all users sudoer permissions allowing an unauthorized user with access to the running container the ability to escalate their own privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2022-38223	There is an out-of-bounds write in checkType located in etc.c in w3m 0.5.3. It can be triggered by sending a crafted HTML file to the w3m binary. It allows an attacker to cause Denial of Service or possibly have unspecified other impact.	7.8	More Details
CVE-2021-39696	In Task.java, there is a possible escalation of privilege due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-185810717	7.8	More Details
CVE-2022-36139	SWFMill commit 53d7690 was discovered to contain a heap-buffer overflow via SWF::Writer::writeByte(unsigned char).	7.8	More Details
CVE-2022-2817	Use After Free in GitHub repository vim/vim prior to 9.0.0213.	7.8	More Details
CVE-2022-20348	In updateState of LocationServicesWifiScanningPreferenceController.java, there is a possible admin restriction 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.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228315529	7.8	More Details
CVE-2022-20349	In WifiScanningPreferenceController and BluetoothScanningPreferenceController, there is a possible admin restriction 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.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228315522	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2819	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.0211.	7.8	More Details
CVE-2022-25793	A Stack-based Buffer Overflow Vulnerability in Autodesk 3ds Max 2022, 2021, and 2020 may lead to code execution through the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer when parsing ActionScript Byte Code files. This vulnerability may allow arbitrary code execution on affected installations of Autodesk 3ds Max.	7.8	More Details
CVE-2021-30490	upsMonitor in ViewPower (aka ViewPowerHTML) 1.04-21012 through 1.04-21353 has insecure permissions for the service binary that enable an Authenticated User to modify files, allowing for privilege escalation.	7.8	More Details
CVE-2022-20360	In setChecked of SecureNfcPreferenceController.java, there is a missing permission check. This could lead to local escalation of privilege from the guest user with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228314987	7.8	More Details
CVE-2022-37393	Zimbra's sudo configuration permits the zimbra user to execute the zmslapd binary as root with arbitrary parameters. As part of its intended functionality, zmslapd can load a user-defined configuration file, which includes plugins in the form of .so files, which also execute as root.	7.8	More Details
CVE-2022-30580	Code injection in Cmd.Start in os/exec before Go 1.17.11 and Go 1.18.3 allows execution of any binaries in the working directory named either "..com" or "..exe" by calling Cmd.Run, Cmd.Start, Cmd.Output, or Cmd.CombinedOutput when Cmd.Path is unset.	7.8	More Details
CVE-2022-20354	In onDefaultNetworkChanged of Vpn.java, there is a possible way to disable VPN due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-219546241	7.8	More Details
CVE-2022-20356	In shouldAllowFgsWhileInUsePermissionLocked of ActiveServices.java, there is a possible way to start foreground service from background 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-11 Android-12 Android-12LAndroid ID: A-215003903	7.8	More Details
CVE-2022-35003	JPEGDEC commit be4843c was discovered to contain a global buffer overflow via ucDitherBuffer at /src/jpeg.inl.	7.8	More Details
CVE-2022-34998	JPEGDEC commit be4843c was discovered to contain a global buffer overflow via JPEGDecodeMCU at /src/jpeg.inl.	7.8	More Details
CVE-2022-34711	Windows Defender Credential Guard Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-35978	Minetest is a free open-source voxel game engine with easy modding and game creation. In **single player**, a mod can set a global setting that controls the Lua script loaded to display the main menu. The script is then loaded as soon as the game session is exited. The Lua environment the menu runs in is not sandboxed and can directly interfere with the user's system. There are currently no known workarounds.	7.7	More Details
CVE-2022-20302	In Settings, there is a possible way to bypass factory reset protections due to a sandbox escape. This could lead to local escalation of privilege if the attacker has physical access to the device, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-200746457	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36524	D-Link GO-RT-AC750 GORTAC750_revA_v101b03 & GO-RT-AC750_revB_FWv200b02 is vulnerable to Static Default Credentials via /etc/init0.d/S80telnetd.sh.	7.5	More Details
CVE-2022-36526	D-Link GO-RT-AC750 GORTAC750_revA_v101b03 & GO-RT-AC750_revB_FWv200b02 is vulnerable to Authentication Bypass via function phpcgi_main in cgibin.	7.5	More Details
CVE-2020-21365	Directory traversal vulnerability in wkhtmltopdf through 0.12.5 allows remote attackers to read local files and disclose sensitive information via a crafted html file running with the default configurations.	7.5	More Details
CVE-2022-28750	Zoom On-Premise Meeting Connector Zone Controller (ZC) before version 4.8.20220419.112 fails to properly parse STUN error codes, which can result in memory corruption and could allow a malicious actor to crash the application. In versions older than 4.8.12.20211115, this vulnerability could also be leveraged to execute arbitrary code.	7.5	More Details
CVE-2022-20408	Product: AndroidVersions: Android kernelAndroid ID: A-204782372References: N/A	7.5	More Details
CVE-2022-20407	Product: AndroidVersions: Android kernelAndroid ID: A-210916981References: N/A	7.5	More Details
CVE-2022-20406	Product: AndroidVersions: Android kernelAndroid ID: A-184676385References: N/A	7.5	More Details
CVE-2022-24949	A privilege escalation to root exists in Eternal Terminal prior to version 6.2.0. This is due to the combination of a race condition, buffer overflow, and logic bug all in PipeSocketHandler::listen().	7.5	More Details
CVE-2022-20404	Product: AndroidVersions: Android kernelAndroid ID: A-205714161References: N/A	7.5	More Details
CVE-2020-23622	An issue in the UPnP protocol in 4thline cling 2.0.0 through 2.1.2 allows remote attackers to cause a denial of service via an unchecked CALLBACK parameter in the request header	7.5	More Details
CVE-2022-33990	Misinterpretation of special domain name characters in dproxy-nexgen (aka dproxy nexgen) leads to cache poisoning because domain names and their associated IP addresses are cached in their misinterpreted form.	7.5	More Details
CVE-2022-33988	dproxy-nexgen (aka dproxy nexgen) re-uses the DNS transaction id (TXID) value from client queries, which allows attackers (able to send queries to the resolver) to conduct DNS cache-poisoning attacks because the TXID value is known to the attacker.	7.5	More Details
CVE-2020-21641	Out-of-Band XML External Entity (OOB-XXE) vulnerability in Zoho ManageEngine Analytics Plus before 4.3.5 allows remote attackers to read arbitrary files, enumerate folders and scan internal ports via crafted XML license file.	7.5	More Details
CVE-2022-20401	In SAEMM_RetrievEPLMNList of SAEMM_ContextManagement.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure post-authentication with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-226446030References: N/A	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33992	DNRD (aka Domain Name Relay Daemon) 2.20.3 forwards and caches DNS queries with the CD (aka checking disabled) bit set to 1. This leads to disabling of DNSSEC protection provided by upstream resolvers.	7.5	More Details
CVE-2022-2832	A flaw was found in Blender 3.3.0. A null pointer dereference exists in source/blender/gpu/opengl/gl_backend.cc that may lead to loss of confidentiality and integrity.	7.5	More Details
CVE-2022-34256	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an Improper Authorization vulnerability that could result in Privilege escalation. An attacker could leverage this vulnerability to access other user's data. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2022-35980	OpenSearch Security is a plugin for OpenSearch that offers encryption, authentication and authorization. Versions 2.0.0.0 and 2.1.0.0 of the security plugin are affected by an information disclosure vulnerability. Requests to an OpenSearch cluster configured with advanced access control features document level security (DLS), field level security (FLS), and/or field masking will not be filtered when the query's search pattern matches an aliased index. OpenSearch Dashboards creates an alias to `.kibana` by default, so filters with the index pattern of `*` to restrict access to documents or fields will not be applied. This issue allows requests to access sensitive information when customer have acted to restrict access that specific information. OpenSearch 2.2.0, which is compatible with OpenSearch Security 2.2.0.0, contains the fix for this issue. There is no recommended work around.	7.5	More Details
CVE-2022-38187	Prior to version 10.9.0, the sharing/rest/content/features/analyze endpoint is always accessible to anonymous users, which could allow an unauthenticated attacker to induce Esri Portal for ArcGIS to read arbitrary URLs.	7.5	More Details
CVE-2022-37041	An issue was discovered in ProxyServlet.java in the /proxy servlet in Zimbra Collaboration Suite (ZCS) 8.8.15 and 9.0. The value of the X-Forwarded-Host header overwrites the value of the Host header in proxied requests. The value of X-Forwarded-Host header is not checked against the whitelist of hosts that ZCS is allowed to proxy to (the zimbraProxyAllowedDomains setting).	7.5	More Details
CVE-2022-35561	A stack overflow vulnerability exists in /goform/WifiMacFilterSet in Tenda W6 V1.0.0.9(4122) version, which can be exploited by attackers to cause a denial of service (DoS) via the index parameter.	7.5	More Details
CVE-2022-35560	A stack overflow vulnerability exists in /goform/wifiSSIDset in Tenda W6 V1.0.0.9(4122) version, which can be exploited by attackers to cause a denial of service (DoS) via the index parameter.	7.5	More Details
CVE-2022-35558	A stack overflow vulnerability exists in /goform/WifiMacFilterGet in Tenda W6 V1.0.0.9(4122) version, which can be exploited by attackers to cause a denial of service (DoS) via the index parameter.	7.5	More Details
CVE-2022-35557	A stack overflow vulnerability exists in /goform/wifiSSIDget in Tenda W6 V1.0.0.9(4122) version, which can be exploited by attackers to cause a denial of service (DoS) via the index parameter.	7.5	More Details
CVE-2022-2833	Endless Infinite loop in Blender-thumnailing due to logical bugs.	7.5	More Details
CVE-2022-2831	A flaw was found in Blender 3.3.0. An interger overflow in source/blender/blendthumb/src/blendthumb_extract.cc may lead to program crash or memory corruption.	7.5	More Details
CVE-2022-24950	A race condition exists in Eternal Terminal prior to version 6.2.0 that allows an authenticated attacker to hijack other users' SSH authorization socket, enabling the attacker to login to other systems as the targeted users. The bug is in UserTerminalRouter::getInfoForId().	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-14322	In Moodle before 3.9.1, 3.8.4, 3.7.7 and 3.5.13, yui_combo needed to limit the amount of files it can load to help mitigate the risk of denial of service.	7.5	More Details
CVE-2022-38184	There is an improper access control vulnerability in Portal for ArcGIS versions 10.8.1 and below which could allow a remote, unauthenticated attacker to access an API that may induce Esri Portal for ArcGIS to read arbitrary URLs.	7.5	More Details
CVE-2022-2379	The Easy Student Results WordPress plugin through 2.2.8 lacks authorisation in its REST API, allowing unauthenticated users to retrieve information related to the courses, exams, departments as well as student's grades and PII such as email address, physical address, phone number etc	7.5	More Details
CVE-2022-35734	'Hulu / フールー' App for Android from version 3.0.47 to the version prior to 3.1.2 uses a hard-coded API key for an external service. By exploiting this vulnerability, API key for an external service may be obtained by analyzing data in the app.	7.5	More Details
CVE-2022-20308	In hostapd, there is a possible insecure configuration due to an insecure default value. This could lead to remote denial of service of the wifi hotspot with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-197874458	7.5	More Details
CVE-2022-2821	Missing Critical Step in Authentication in GitHub repository namelessmc/nameless prior to v2.0.2.	7.5	More Details
CVE-2022-2822	An attacker can freely brute force username and password and can takeover any account. An attacker could easily guess user passwords and gain access to user and administrative accounts.	7.5	More Details
CVE-2022-33939	CENTUM VP / CS 3000 controller FCS (CP31, CP33, CP345, CP401, and CP451) contains an issue in processing communication packets, which may lead to resource consumption. If this vulnerability is exploited, an attacker may cause a denial of service (DoS) condition in ADL communication by sending a specially crafted packet to the affected product.	7.5	More Details
CVE-2022-38216	An integer overflow exists in Mapbox's closed source gl-native library prior to version 10.6.1, which is bundled with multiple Mapbox products including open source libraries. The overflow is caused by large image height and width values when creating a new Image and allows for out of bounds writes, potentially crashing the Mapbox process.	7.5	More Details
CVE-2022-37423	Neo4j APOC (Awesome Procedures on Cypher) before 4.3.0.7 and 4.x before 4.4.0.8 allows Directory Traversal to sibling directories via apoc.log.stream.	7.5	More Details
CVE-2021-42052	IPESA e-Flow 3.3.6 allows path traversal for reading any file within the web root directory via the lib/js/build/STEResource.res path and the R query parameter.	7.5	More Details
CVE-2022-37006	Permission control vulnerability in the network module. Successful exploitation of this vulnerability may affect service availability.	7.5	More Details
CVE-2022-30630	Uncontrolled recursion in Glob in io/fs before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a path which contains a large number of path separators.	7.5	More Details
CVE-2022-29804	Incorrect conversion of certain invalid paths to valid, absolute paths in Clean in path/filepath before Go 1.17.11 and Go 1.18.3 on Windows allows potential directory traversal attack.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34661	A vulnerability has been identified in Teamcenter V12.4 (All versions < V12.4.0.15), Teamcenter V13.0 (All versions < V13.0.0.10), Teamcenter V13.1 (All versions < V13.1.0.10), Teamcenter V13.2 (All versions < V13.2.0.9), Teamcenter V13.3 (All versions < V13.3.0.5), Teamcenter V14.0 (All versions < V14.0.0.2). File Server Cache service in Teamcenter is vulnerable to denial of service by entering infinite loops and using up CPU cycles. This could allow an attacker to cause denial of service condition.	7.5	More Details
CVE-2022-28131	Uncontrolled recursion in Decoder.Skip in encoding/xml before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a deeply nested XML document.	7.5	More Details
CVE-2022-37001	The diag-router module has a vulnerability in intercepting excessive long and short instructions. Successful exploitation of this vulnerability will cause the diag-router module to crash.	7.5	More Details
CVE-2022-37004	The Settings application has a vulnerability of bypassing the out-of-box experience (OOBE). Successful exploitation of this vulnerability may affect the availability.	7.5	More Details
CVE-2022-20247	In Media, 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 not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-229858836	7.5	More Details
CVE-2022-37005	The Settings application has an argument injection vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-34659	A vulnerability has been identified in Simcenter STAR-CCM+ (All versions only if the Power-on-Demand public license server is used). Affected applications expose user, host and display name of users, when the public license server is used. This could allow an attacker to retrieve this information.	7.5	More Details
CVE-2022-37007	The chinadrm module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may affect the availability.	7.5	More Details
CVE-2022-37008	The recovery module has a vulnerability of bypassing the verification of an update package before use. Successful exploitation of this vulnerability may affect system stability.	7.5	More Details
CVE-2022-38150	In Varnish Cache 7.0.0, 7.0.1, 7.0.2, and 7.1.0, it is possible to cause the Varnish Server to assert and automatically restart through forged HTTP/1 backend responses. An attack uses a crafted reason phrase of the backend response status line. This is fixed in 7.0.3 and 7.1.1.	7.5	More Details
CVE-2022-38155	TEE_Malloc in Samsung mTower through 0.3.0 allows a trusted application to achieve Excessive Memory Allocation via a large len value, as demonstrated by a Numaker-PFM-M2351 TEE kernel crash.	7.5	More Details
CVE-2022-38161	The Gumstix Overo SBC on the VSKS board through 2022-08-09, as used on the Orlan-10 and other platforms, allows unrestricted remapping of the NOR flash memory containing the bitstream for the FPGA.	7.5	More Details
CVE-2022-36324	Affected devices do not properly handle the renegotiation of SSL/TLS parameters. This could allow an unauthenticated remote attacker to bypass the TCP brute force prevention and lead to a denial of service condition for the duration of the attack.	7.5	More Details
CVE-2021-40040	Vulnerability of writing data to an arbitrary address in the HW_KEYMASTER module. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40034	The video framework has the memory overwriting vulnerability caused by addition overflow. Successful exploitation of this vulnerability may affect the availability.	7.5	More Details
CVE-2022-20244	In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if more than 100 bluetooth devices have been connected with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-201083240	7.5	More Details
CVE-2021-40030	The My HUAWEI app has a defect in the design. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2021-33646	The th_read() function doesn’t free a variable t->th_buf.gnu_longname after allocating memory, which may cause a memory leak.	7.5	More Details
CVE-2021-33645	The th_read() function doesn’t free a variable t->th_buf.gnu_longlink after allocating memory, which may cause a memory leak.	7.5	More Details
CVE-2022-35715	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in a stack trace. This information could be used in further attacks against the system. IBM X-Force ID: 231202.	7.5	More Details
CVE-2021-46304	A vulnerability has been identified in CP-8000 MASTER MODULE WITH I/O -25/+70°C (All versions), CP-8000 MASTER MODULE WITH I/O -40/+70°C (All versions), CP-8021 MASTER MODULE (All versions), CP-8022 MASTER MODULE WITH GPRS (All versions). The component allows to activate a web server module which provides unauthenticated access to its web pages. This could allow an attacker to retrieve debug-level information from the component such as internal network topology or connected systems.	7.5	More Details
CVE-2022-36923	Zoho ManageEngine OpManager, OpManager Plus, OpManager MSP, Network Configuration Manager, NetFlow Analyzer, Firewall Analyzer, and OpUtils before 2022-07-27 through 2022-07-28 (125657, 126002, 126104, and 126118) allow unauthenticated attackers to obtain a user's API key, and then access external APIs.	7.5	More Details
CVE-2021-37150	Improper Input Validation vulnerability in header parsing of Apache Traffic Server allows an attacker to request secure resources. This issue affects Apache Traffic Server 8.0.0 to 9.1.2.	7.5	More Details
CVE-2022-31779	Improper Input Validation vulnerability in HTTP/2 header parsing of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 9.1.2.	7.5	More Details
CVE-2022-20375	In LteRrcNrProAsnDecode of LteRrcNr_Codec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-180956894References: N/A	7.5	More Details
CVE-2022-20380	Product: AndroidVersions: Android kernelAndroid ID: A-212625740References: N/A	7.5	More Details
CVE-2022-25763	Improper Input Validation vulnerability in HTTP/2 request validation of Apache Traffic Server allows an attacker to create smuggle or cache poison attacks. This issue affects Apache Traffic Server 8.0.0 to 9.1.2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32189	A too-short encoded message can cause a panic in Float.GobDecode and Rat GobDecode in math/big in Go before 1.17.13 and 1.18.5, potentially allowing a denial of service.	7.5	More Details
CVE-2022-28129	Improper Input Validation vulnerability in HTTP/1.1 header parsing of Apache Traffic Server allows an attacker to send invalid headers. This issue affects Apache Traffic Server 8.0.0 to 9.1.2.	7.5	More Details
CVE-2022-35290	Under certain conditions SAP Authenticator for Android allows an attacker to access information which would otherwise be restricted.	7.5	More Details
CVE-2022-20370	Product: AndroidVersions: Android kernelAndroid ID: A-215730643References: N/A	7.5	More Details
CVE-2022-31778	Improper Input Validation vulnerability in handling the Transfer-Encoding header of Apache Traffic Server allows an attacker to poison the cache. This issue affects Apache Traffic Server 8.0.0 to 9.0.2.	7.5	More Details
CVE-2022-30635	Uncontrolled recursion in Decoder.Decode in encoding/gob before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a message which contains deeply nested structures.	7.5	More Details
CVE-2022-31675	VMware vRealize Operations contains an authentication bypass vulnerability. An unauthenticated malicious actor with network access may be able to create a user with administrative privileges.	7.5	More Details
CVE-2022-30632	Uncontrolled recursion in Glob in path/filepath before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via a path containing a large number of path separators.	7.5	More Details
CVE-2022-30631	Uncontrolled recursion in Reader.Read in compress/gzip before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via an archive containing a large number of concatenated 0-length compressed files.	7.5	More Details
CVE-2022-30633	Uncontrolled recursion in Unmarshal in encoding/xml before Go 1.17.12 and Go 1.18.4 allows an attacker to cause a panic due to stack exhaustion via unmarshalling an XML document into a Go struct which has a nested field that uses the 'any' field tag.	7.5	More Details
CVE-2022-31780	Improper Input Validation vulnerability in HTTP/2 frame handling of Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 8.0.0 to 9.1.2.	7.5	More Details
CVE-2022-28636	A potential local arbitrary code execution and a local denial of service (DoS) vulnerability within an isolated process were discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Prior to 2.71. An unprivileged user could locally exploit this vulnerability to potentially execute arbitrary code in an isolated process resulting in a complete loss of confidentiality, integrity, and availability within that process. In addition, an unprivileged user could exploit a denial of service (DoS) vulnerability in an isolated process resulting in a complete loss of availability within that process. A successful attack depends on conditions beyond the attackers control. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 5 (iLO 5).	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20866	A vulnerability in the handling of RSA keys on devices running Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to retrieve an RSA private key. This vulnerability is due to a logic error when the RSA key is stored in memory on a hardware platform that performs hardware-based cryptography. An attacker could exploit this vulnerability by using a Lenstra side-channel attack against the targeted device. A successful exploit could allow the attacker to retrieve the RSA private key. The following conditions may be observed on an affected device: This vulnerability will apply to approximately 5 percent of the RSA keys on a device that is running a vulnerable release of Cisco ASA Software or Cisco FTD Software; not all RSA keys are expected to be affected due to mathematical calculations applied to the RSA key. The RSA key could be valid but have specific characteristics that make it vulnerable to the potential leak of the RSA private key. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic. See the Indicators of Compromise section for more information on the detection of this type of RSA key. The RSA key could be malformed and invalid. A malformed RSA key is not functional, and a TLS client connection to a device that is running Cisco ASA Software or Cisco FTD Software that uses the malformed RSA key will result in a TLS signature failure, which means a vulnerable software release created an invalid RSA signature that failed verification. If an attacker obtains the RSA private key, they could use the key to impersonate a device that is running Cisco ASA Software or Cisco FTD Software or to decrypt the device traffic.	7.4	More Details
CVE-2022-37437	When using Ingest Actions to configure a destination that resides on Amazon Simple Storage Service (S3) in Splunk Web, TLS certificate validation is not correctly performed and tested for the destination. The vulnerability only affects connections between Splunk Enterprise and an Ingest Actions Destination through Splunk Web and only applies to environments that have configured TLS certificate validation. It does not apply to Destinations configured directly in the outputs.conf configuration file. The vulnerability affects Splunk Enterprise version 9.0.0 and does not affect versions below 9.0.0, including the 8.1.x and 8.2.x versions.	7.4	More Details
CVE-2022-28635	A potential local arbitrary code execution and a local denial of service (DoS) vulnerability within an isolated process were discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Prior to 2.71. An unprivileged user could locally exploit this vulnerability to potentially execute arbitrary code in an isolated process resulting in a complete loss of confidentiality, integrity, and availability within that process. In addition, an unprivileged user could exploit a denial of service (DoS) vulnerability in an isolated process resulting in a complete loss of availability within that process. A successful attack depends on conditions beyond the attackers control. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 5 (iLO 5).	7.4	More Details
CVE-2022-2802	A vulnerability has been found in SourceCodester Gas Agency Management System and classified as critical. This vulnerability affects unknown code of the file gasmark/login.php. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-206248.	7.3	More Details
CVE-2022-28630	A local arbitrary code execution vulnerability was discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Prior to 2.71. An unprivileged user could locally exploit this vulnerability to execute arbitrary code resulting in a complete loss of confidentiality and integrity, and a partial loss of availability. User interaction is required to exploit this vulnerability. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 5 (iLO 5).	7.3	More Details
CVE-2022-30575	The Web Console component of TIBCO Software Inc.'s TIBCO Data Science - Workbench, TIBCO Statistica, TIBCO Statistica - Estore Edition, and TIBCO Statistica Trial contains easily exploitable Reflected Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker with network access to execute scripts targeting the affected system or the victim's local system. Affected releases are TIBCO Software Inc.'s TIBCO Data Science - Workbench: versions 14.0.0 and below, TIBCO Statistica: versions 14.0.0 and below, TIBCO Statistica - Estore Edition: versions 14.0.0 and below, and TIBCO Statistica Trial: versions 14.0.0 and below.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2766	A vulnerability was found in SourceCodester Loan Management System. It has been rated as critical. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument password leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-206162 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2022-28633	A local disclosure of sensitive information and a local unauthorized data modification vulnerability were discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Prior to 2.71. An unprivileged user could locally exploit this vulnerability to read and write to the iLO 5 firmware file system resulting in a complete loss of confidentiality and a partial loss of integrity and availability. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 5 (iLO 5).	7.3	More Details
CVE-2022-2812	A vulnerability classified as critical was found in SourceCodester Guest Management System. This vulnerability affects unknown code of the file index.php. The manipulation of the argument username/pass leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-206398 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2022-36293	Buffer overflow vulnerability in Nintendo Wi-Fi Network Adaptor WAP-001 All versions allows an attacker with an administrative privilege to execute arbitrary code via unspecified vectors.	7.2	More Details
CVE-2020-1756	In Moodle before 3.8.2, 3.7.5, 3.6.9 and 3.5.11, insufficient input escaping was applied to the PHP unit webrunner admin tool.	7.2	More Details
CVE-2022-36381	OS command injection vulnerability in Nintendo Wi-Fi Network Adaptor WAP-001 All versions allows an attacker with an administrative privilege to execute arbitrary OS commands via unspecified vectors.	7.2	More Details
CVE-2022-34253	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an XML Injection vulnerability in the Widgets Module. An attacker with admin privileges can trigger a specially crafted script to achieve remote code execution. Exploitation of this issue does not require user interaction.	7.2	More Details
CVE-2022-31672	VMware vRealize Operations contains a privilege escalation vulnerability. A malicious actor with administrative network access can escalate privileges to root.	7.2	More Details
CVE-2022-2354	The WP-DBManager WordPress plugin before 2.80.8 does not prevent administrators from running arbitrary commands on the server in multisite installations, where only super-administrators should.	7.2	More Details
CVE-2021-44720	In Ivanti Pulse Secure Pulse Connect Secure (PCS) before 9.1R12, the administrator password is stored in the HTML source code of the "Maintenance > Push Configuration > Targets > Target Name" targets.cgi screen. A read-only administrative user can escalate to a read-write administrative role.	7.2	More Details
CVE-2022-22369	IBM Workload Scheduler 9.4 and 9.5 could allow a local user to overwrite key system files which would cause the system to crash. IBM X-Force ID: 221187.	7.1	More Details
CVE-2022-28754	Zoom On-Premise Meeting Connector MMR before version 4.8.129.20220714 contains an improper access control vulnerability. As a result, a malicious actor can join a meeting which they are authorized to join without appearing to the other participants, can admit themselves into the meeting from the waiting room, and can become host and cause other meeting disruptions.	7.1	More Details
CVE-2022-28753	Zoom On-Premise Meeting Connector MMR before version 4.8.129.20220714 contains an improper access control vulnerability. As a result, a malicious actor can join a meeting which they are authorized to join without appearing to the other participants, can admit themselves into the meeting from the waiting room, and can become host and cause other meeting disruptions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33926	Dell Wyse Management Suite 3.6.1 and below contains an improper access control vulnerability. A remote malicious user could exploit this vulnerability in order to retain access to a file repository after it has been revoked.	7.1	More Details
CVE-2022-35822	Windows Defender Credential Guard Security Feature Bypass Vulnerability	7.1	More Details
CVE-2022-35953	BookWyrm is a social network for tracking your reading, talking about books, writing reviews, and discovering what to read next. Some links in BookWyrm may be vulnerable to tabnabbing, a form of phishing that gives attackers an opportunity to redirect a user to a malicious site. The issue was patched in version 0.4.5.	7.1	More Details
CVE-2022-2820	Session Fixation in GitHub repository namelessmc/nameless prior to v2.0.2.	7.0	More Details
CVE-2022-24951	A race condition exists in Eternal Terminal prior to version 6.2.0 which allows a local attacker to hijack Eternal Terminal's IPC socket, enabling access to Eternal Terminal clients which attempt to connect in the future.	7.0	More Details
CVE-2022-20344	In stealReceiveChannel of EventThread.cpp, there is a possible way to interfere with process communication due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-232541124	7.0	More Details
CVE-2022-2503	Dm-verity is used for extending root-of-trust to root filesystems. LoadPin builds on this property to restrict module/firmware loads to just the trusted root filesystem. Device-mapper table reloads currently allow users with root privileges to switch out the target with an equivalent dm-linear target and bypass verification till reboot. This allows root to bypass LoadPin and can be used to load untrusted and unverified kernel modules and firmware, which implies arbitrary kernel execution and persistence for peripherals that do not verify firmware updates. We recommend upgrading past commit 4caae58406f8ceb741603eee460d79bacca9b1b5	6.9	More Details
CVE-2022-36307	The AirVelocity 1500 prints SNMP credentials on its physically accessible serial port during boot. This was fixed in AirVelocity 1500 software version 15.18.00.2511 and may affect other AirVelocity and AirSpeed models.	6.8	More Details
CVE-2022-20269	In Bluetooth, there is a possible out of bounds write 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.Product: AndroidVersions: Android-13Android ID: A-209062898	6.8	More Details
CVE-2022-20313	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 System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-192206329	6.8	More Details
CVE-2022-36325	Affected devices do not properly sanitize data introduced by an user when rendering the web interface. This could allow an authenticated remote attacker with administrative privileges to inject code and lead to a DOM-based XSS.	6.8	More Details
CVE-2022-38194	In Esri Portal for ArcGIS versions 10.8.1, a system property is not properly encrypted. This may lead to a local user reading sensitive information from a properties file.	6.7	More Details
CVE-2022-28626	A local arbitrary code execution vulnerability was discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Prior to 2.71. A highly privileged user could locally exploit this vulnerability to execute arbitrary code resulting in a complete loss of confidentiality, integrity, and availability. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 5 (iLO 5).	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28634	A local arbitrary code execution vulnerability was discovered in HPE Integrated Lights-Out 5 (iLO 5) firmware version(s): Prior to 2.71. A highly privileged user could locally exploit this vulnerability to execute arbitrary code resulting in a complete loss of confidentiality, integrity, and availability. HPE has provided a firmware update to resolve this vulnerability in HPE Integrated Lights-Out 5 (iLO 5).	6.7	More Details
CVE-2022-20314	In KeyChain, there is a possible spoof keychain chooser activity request due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-191876118	6.7	More Details
CVE-2022-20306	In Camera Provider HAL, there is a possible memory corruption 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.Product: AndroidVersions: Android-13Android ID: A-199680794	6.7	More Details
CVE-2022-20382	In (TBD) of (TBD), there is a possible out of bounds write due to kernel stack overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-214245176References: Upstream kernel	6.7	More Details
CVE-2022-20366	In ioctl_dpm_clk_update of lwis_ioctl.c, there is a possible out of bounds write 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.Product: AndroidVersions: Android kernelAndroid ID: A-225877745References: N/A	6.7	More Details
CVE-2022-20158	In bdi_put and bdi_unregister of backing-dev.c, there is a possible memory corruption 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.Product: AndroidVersions: Android kernelAndroid ID: A-182815710References: Upstream kernel	6.7	More Details
CVE-2022-20379	In lwis_buffer_alloc of lwis_buffer.c, there is a possible arbitrary code execution 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.Product: AndroidVersions: Android kernelAndroid ID: A-209436980References: N/A	6.7	More Details
CVE-2022-20377	In TBD of keymaster_ipc.cpp, there is a possible to force gatekeeper, fingerprint, and faceauth to use a known HMAC key. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-222339795References: N/A	6.7	More Details
CVE-2022-20376	In trusty_log_seq_start of trusty-log.c, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-216130110References: N/A	6.7	More Details
CVE-2022-20372	In exynos5_i2c_irq of (TBD), there is a possible out of bounds write 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.Product: AndroidVersions: Android kernelAndroid ID: A-195480799References: N/A	6.7	More Details
CVE-2022-20369	In v4l2_m2m_querybuf of v4l2-mem2mem.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-223375145References: Upstream kernel	6.7	More Details
CVE-2022-20367	In construct_transaction of lwis_ioctl.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-225877459References: N/A	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1705	Acceptance of some invalid Transfer-Encoding headers in the HTTP/1 client in net/http before Go 1.17.12 and Go 1.18.4 allows HTTP request smuggling if combined with an intermediate server that also improperly fails to reject the header as invalid.	6.5	More Details
CVE-2022-35473	OTFCC v0.10.4 was discovered to contain a segmentation violation via /release-x64/otfccdump+0x4fe9a7.	6.5	More Details
CVE-2022-20346	In updateAudioTrackInfoFromESDS_MPEG4Audio of MPEG4Extractor.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-230493653	6.5	More Details
CVE-2022-35012	PNGDec commit 8abf6be was discovered to contain a heap buffer overflow via SaveBMP at /linux/main.cpp.	6.5	More Details
CVE-2022-2605	Out of bounds read in Dawn in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	6.5	More Details
CVE-2022-35474	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b544e.	6.5	More Details
CVE-2022-35475	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6e41a8.	6.5	More Details
CVE-2022-35471	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6e41b0.	6.5	More Details
CVE-2022-35472	OTFCC v0.10.4 was discovered to contain a global overflow via /release-x64/otfccdump+0x718693.	6.5	More Details
CVE-2022-20273	In Bluetooth, 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 not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-206478022	6.5	More Details
CVE-2022-35470	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x65fc97.	6.5	More Details
CVE-2022-35010	PNGDec commit 8abf6be was discovered to contain a heap buffer overflow via asan_interceptors_memintrinsics.cpp.	6.5	More Details
CVE-2022-36306	An authenticated attacker can enumerate and download sensitive files, including the eNodeB's web management UI's TLS private key, the web server binary, and the web server configuration file. These vulnerabilities were found in AirVelocity 1500 running software version 9.3.0.01249, were still present in 15.18.00.2511, and may affect other AirVelocity and AirSpeed models.	6.5	More Details
CVE-2022-35477	OTFCC v0.10.4 was discovered to contain a segmentation violation via /release-x64/otfccdump+0x4fe954.	6.5	More Details
CVE-2022-35469	OTFCC v0.10.4 was discovered to contain a segmentation violation via /x86_64-linux-gnu/libc.so.6+0xbb384.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35468	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6e420d.	6.5	More Details
CVE-2022-35467	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6e41b8.	6.5	More Details
CVE-2022-35476	OTFCC v0.10.4 was discovered to contain a segmentation violation via /release-x64/otfccdump+0x4fbc0b.	6.5	More Details
CVE-2022-35479	OTFCC v0.10.4 was discovered to contain a segmentation violation via /release-x64/otfccdump+0x4fbbb6.	6.5	More Details
CVE-2022-2610	Insufficient policy enforcement in Background Fetch in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2022-2622	Insufficient validation of untrusted input in Safe Browsing in Google Chrome on Windows prior to 104.0.5112.79 allowed a remote attacker to bypass download restrictions via a crafted file.	6.5	More Details
CVE-2022-20816	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to delete arbitrary files from an affected system. This vulnerability exists because the affected software does not properly validate HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected software. A successful exploit could allow the attacker to delete arbitrary files from the affected system.	6.5	More Details
CVE-2022-38183	In Gitea before 1.16.9, it was possible for users to add existing issues to projects. Due to improper access controls, an attacker could assign any issue to any project in Gitea (there was no permission check for fetching the issue). As a result, the attacker would get access to private issue titles.	6.5	More Details
CVE-2022-35486	OTFCC v0.10.4 was discovered to contain a segmentation violation via /release-x64/otfccdump+0x6badae.	6.5	More Details
CVE-2022-35485	OTFCC v0.10.4 was discovered to contain a segmentation violation via /release-x64/otfccdump+0x703969.	6.5	More Details
CVE-2022-20253	In Bluetooth, there is a possible cleanup failure due to an uncaught exception. This could lead to remote denial of service in Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-224545125	6.5	More Details
CVE-2022-23238	Linux deployments of StorageGRID (formerly StorageGRID Webscale) versions 11.6.0 through 11.6.0.2 deployed with a Linux kernel version less than 4.7.0 are susceptible to a vulnerability which could allow a remote unauthenticated attacker to view limited metrics information and modify alert email recipients and content.	6.5	More Details
CVE-2022-35484	OTFCC v0.10.4 was discovered to contain a segmentation violation via /release-x64/otfccdump+0x6b6a8f.	6.5	More Details
CVE-2022-35483	OTFCC v0.10.4 was discovered to contain a segmentation violation via /release-x64/otfccdump+0x5266a8.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2612	Side-channel information leakage in Keyboard input in Google Chrome prior to 104.0.5112.79 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page.	6.5	More Details
CVE-2022-35482	OTFCC v0.10.4 was discovered to contain a segmentation violation via /release-x64/otfccdump+0x65f724.	6.5	More Details
CVE-2022-2618	Insufficient validation of untrusted input in Internals in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to bypass download restrictions via a malicious file .	6.5	More Details
CVE-2022-35481	OTFCC v0.10.4 was discovered to contain a segmentation violation via /multiarch/memmove-vec-unaligned-erms.S.	6.5	More Details
CVE-2022-2616	Inappropriate implementation in Extensions API in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to spoof the contents of the Omnibox (URL bar) via a crafted Chrome Extension.	6.5	More Details
CVE-2022-2615	Insufficient policy enforcement in Cookies in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2022-35465	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6c0414.	6.5	More Details
CVE-2022-35478	OTFCC v0.10.4 was discovered to contain a segmentation violation via /release-x64/otfccdump+0x6babea.	6.5	More Details
CVE-2022-35466	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6c0473.	6.5	More Details
CVE-2022-24952	Several denial of service vulnerabilities exist in Eternal Terminal prior to version 6.2.0, including a DoS triggered remotely by an invalid sequence number and a local bug triggered by invalid input sent directly to the IPC socket.	6.5	More Details
CVE-2022-35464	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6171b2.	6.5	More Details
CVE-2022-35449	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b0466.	6.5	More Details
CVE-2021-39087	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.5, 6.1.0.0 through 6.1.0.4, and 6.1.1.0 through 6.1.1.1 could allow an authenticated user to obtain sensitive information due to improper permission controls. IBM X-Force ID: 216109.	6.5	More Details
CVE-2022-33925	Dell Wyse Management Suite 3.6.1 and below contains an Improper Access control vulnerability in UI. An remote authenticated attacker could potentially exploit this vulnerability by bypassing access controls in order to download reports containing sensitive information.	6.5	More Details
CVE-2022-32148	Improper exposure of client IP addresses in net/http before Go 1.17.12 and Go 1.18.4 can be triggered by calling httputil.ReverseProxy.ServeHTTP with a Request.Header map containing a nil value for the X-Forwarded-For header, which causes ReverseProxy to set the client IP as the value of the X-Forwarded-For header.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22411	IBM Spectrum Scale Data Access Services (DAS) 5.1.3.1 could allow an authenticated user to insert code which could allow the attacker to manipulate cluster resources due to excessive permissions. IBM X-Force ID: 223016.	6.5	More Details
CVE-2022-35453	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6c08a6.	6.5	More Details
CVE-2022-35452	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b0b2c.	6.5	More Details
CVE-2022-35451	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b03b5.	6.5	More Details
CVE-2022-35450	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b84b1.	6.5	More Details
CVE-2022-35448	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b55af.	6.5	More Details
CVE-2022-35456	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x617087.	6.5	More Details
CVE-2022-2756	Server-Side Request Forgery (SSRF) in GitHub repository kareadita/kavita prior to 0.5.4.1.	6.5	More Details
CVE-2022-35447	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b04de.	6.5	More Details
CVE-2022-35433	ffjpeg commit caade60a69633d74100bd3c2528bddee0b6a1291 was discovered to contain a memory leak via /src/jfif.c.	6.5	More Details
CVE-2022-35100	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via gfxline_getbbox at /lib/gfxtools.c.	6.5	More Details
CVE-2022-35013	PNGDec commit 8abf6be was discovered to contain a FPE via SaveBMP at /linux/main.cpp.	6.5	More Details
CVE-2022-35007	PNGDec commit 8abf6be was discovered to contain a heap buffer overflow via __interceptor_fwrite.part.57 at sanitizer_common_interceptors.inc.	6.5	More Details
CVE-2022-35008	PNGDec commit 8abf6be was discovered to contain a stack overflow via /linux/main.cpp.	6.5	More Details
CVE-2022-35009	PNGDec commit 8abf6be was discovered to contain a memory allocation problem via asan_malloc_linux.cpp.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35454	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b05aa.	6.5	More Details
CVE-2022-35455	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b0d63.	6.5	More Details
CVE-2022-20334	In Bluetooth, there are possible process crashes due to dereferencing a null pointer. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-178800552	6.5	More Details
CVE-2022-35459	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6e412a.	6.5	More Details
CVE-2022-35463	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b0478.	6.5	More Details
CVE-2022-35461	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6c0a32.	6.5	More Details
CVE-2022-35460	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x61731f.	6.5	More Details
CVE-2022-34365	WMS 3.7 contains a Path Traversal Vulnerability in Device API. An attacker could potentially exploit this vulnerability, to gain unauthorized read access to the files stored on the server filesystem, with the privileges of the running web application.	6.5	More Details
CVE-2022-35458	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6b05ce.	6.5	More Details
CVE-2022-20333	In Bluetooth, there is a possible crash due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-179161657	6.5	More Details
CVE-2022-35462	OTFCC v0.10.4 was discovered to contain a heap-buffer overflow via /release-x64/otfccdump+0x6c0bc3.	6.5	More Details
CVE-2022-20373	In st21nfc_loc_set_polaritymode of fc/st21nfc.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-208269510References: N/A	6.4	More Details
CVE-2022-20371	In dm_bow_dtr and related functions of dm-bow.c, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-195565510References: Upstream kernel	6.4	More Details
CVE-2022-20256	In the Audio HAL, there is a possible out of bounds write due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-222572821	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33928	Dell Wyse Management Suite 3.6.1 and below contains an Plain-text Password Storage Vulnerability in UI. An attacker with low privileges could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	6.4	More Details
CVE-2022-2801	A vulnerability, which was classified as critical, was found in SourceCodester Automated Beer Parlour Billing System. This affects an unknown part of the component Login. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-206247.	6.3	More Details
CVE-2022-33931	Dell Wyse Management Suite 3.6.1 and below contains an Improper Access control vulnerability in UI. An attacker with no access to Alert Classification page could potentially exploit this vulnerability, leading to the change the alert categories.	6.3	More Details
CVE-2022-2744	A vulnerability, which was classified as critical, has been found in SourceCodester Gym Management System. Affected by this issue is some unknown functionality of the file /admin/add_exercises.php of the component Background Management. The manipulation of the argument exer_img leads to unrestricted upload. The attack may be launched remotely. The identifier of this vulnerability is VDB-206012.	6.3	More Details
CVE-2022-2803	A vulnerability was found in SourceCodester Zoo Management System and classified as critical. This issue affects some unknown processing of the file /pages/animals.php. The manipulation of the argument class_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-206249 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2804	A vulnerability was found in SourceCodester Zoo Management System. It has been classified as critical. Affected is an unknown function of the file /pages/apply_vacancy.php. The manipulation of the argument filename leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-206250 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-2751	A vulnerability was found in SourceCodester Company Website CMS and classified as critical. Affected by this issue is some unknown functionality of the file /dashboard/add-portfolio.php. The manipulation of the argument ufile leads to unrestricted upload. The attack may be launched remotely. The identifier of this vulnerability is VDB-206024.	6.3	More Details
CVE-2022-2779	A vulnerability classified as critical was found in SourceCodester Gas Agency Management System. Affected by this vulnerability is an unknown functionality of the file /gasmark/assets/myimages/oneWord.php. The manipulation of the argument shell leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-206173 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2747	A vulnerability was found in SourceCodester Simple Online Book Store and classified as critical. This issue affects some unknown processing of the file book.php. The manipulation of the argument book_isbn leads to sql injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-206015.	6.3	More Details
CVE-2022-2746	A vulnerability has been found in SourceCodester Simple Online Book Store System and classified as critical. This vulnerability affects unknown code of the file Admin_ add.php. The manipulation leads to unrestricted upload. The attack can be initiated remotely. VDB-206014 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-2750	A vulnerability, which was classified as critical, was found in SourceCodester Company Website CMS. Affected is an unknown function of the file /dashboard/add-service.php of the component Add Service Handler. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. VDB-206022 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2847	A vulnerability, which was classified as critical, has been found in SourceCodester Guest Management System. This issue affects some unknown processing of the file /guestmanagement/front.php. The manipulation of the argument rid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-206489 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2772	A vulnerability was found in SourceCodester Apartment Visitor Management System and classified as critical. Affected by this issue is some unknown functionality of the file action-visitor.php. The manipulation of the argument editid/remark leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-206168.	6.3	More Details
CVE-2022-2765	A vulnerability was found in SourceCodester Company Website CMS 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /dashboard/settings. The manipulation leads to improper authentication. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-206161 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2745	A vulnerability, which was classified as critical, was found in SourceCodester Gym Management System. This affects an unknown part of the file /admin/add_trainers.php of the component Add New Trainer. The manipulation of the argument trainer_name leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-206013 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2771	A vulnerability has been found in SourceCodester Simple Online Book Store System and classified as critical. Affected by this vulnerability is an unknown functionality of the file /obs/bookPerPub.php. The manipulation of the argument bookisbn leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-206167.	6.3	More Details
CVE-2022-2770	A vulnerability, which was classified as critical, was found in SourceCodester Simple Online Book Store System. Affected is an unknown function of the file /obs/book.php. The manipulation of the argument bookisbn leads to sql injection. It is possible to launch the attack remotely. VDB-206166 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-2736	A vulnerability was found in SourceCodester Company Website CMS. It has been classified as critical. This affects an unknown part of the file /dashboard/updatelogo.php of the component Background Upload Logo Icon. The manipulation of the argument xfile/ufile leads to unrestricted upload. It is possible to initiate the attack remotely. The identifier VDB-205881 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2740	A vulnerability was found in SourceCodester Company Website CMS. It has been declared as critical. This vulnerability affects unknown code of the file /dashboard/add-blog.php of the component Add Blog. The manipulation of the argument ufile leads to unrestricted upload. The attack can be initiated remotely. VDB-205882 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-2797	A vulnerability classified as critical was found in SourceCodester Student Information System. Affected by this vulnerability is an unknown functionality of the file /admin/students/view_student.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The identifier VDB-206245 was assigned to this vulnerability.	6.3	More Details
CVE-2022-2774	A vulnerability was found in SourceCodester Library Management System. It has been declared as critical. This vulnerability affects unknown code of the file librarian/student.php. The manipulation of the argument title leads to sql injection. The attack can be initiated remotely. VDB-206170 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-25799	An open redirect vulnerability exists in CERT/CC VINCE software prior to 1.50.0. An attacker could send a link that has a specially crafted URL and convince the user to click the link. When an authenticated user clicks the link, the authenticated user's browser could be redirected to a malicious site that is designed to impersonate a legitimate website. The attacker could trick the user and potentially acquire sensitive information such as the user's credentials.	6.1	More Details
CVE-2022-36311	Airspan AirVelocity 1500 prior to software version 15.18.00.2511 is vulnerable to injection leading to XSS in the SNMP community field in the eNodeB's web management UI. This issue may affect other AirVelocity and AirSpeed models.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36007	Venice is a Clojure inspired sandboxed Lisp dialect with excellent Java interoperability. A partial path traversal issue exists within the functions `load-file` and `load-resource`. These functions can be limited to load files from a list of load paths. Assuming Venice has been configured with the load paths: `[ "/Users/foo/resources" ]` When passing **relative** paths to these two vulnerable functions everything is fine: `(load-resource "test.png")` => loads the file "/Users/foo/resources/test.png" `(load-resource "../resources-alt/test.png")` => rejected, outside the load path When passing **absolute** paths to these two vulnerable functions Venice may return files outside the configured load paths: `(load-resource "/Users/foo/resources/test.png")` => loads the file "/Users/foo/resources/test.png" `(load-resource "/Users/foo/resources-alt/test.png")` => loads the file "/Users/foo/resources-alt/test.png" !!! The latter call suffers from the _Partial Path Traversal_ vulnerability. This issue's scope is limited to absolute paths whose name prefix matches a load path. E.g. for a load-path `"/Users/foo/resources"`, the actor can cause loading a resource also from `"/Users/foo/resources-alt"`, but not from `"/Users/foo/images"`. Versions of Venice before and including v1.10.17 are affected by this issue. Upgrade to Venice >= 1.10.18, if you are on a version < 1.10.18. There are currently no known workarounds.	6.1	More Details
CVE-2022-38190	A stored Cross Site Scripting (XSS) vulnerability in Esri Portal for ArcGIS configurable apps may allow a remote, unauthenticated attacker to pass and store malicious strings via crafted queries which when accessed could potentially execute arbitrary JavaScript code in the user's browser	6.1	More Details
CVE-2022-34257	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	6.1	More Details
CVE-2022-20869	A vulnerability in the web-based management interface of Cisco BroadWorks Application Delivery Platform Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.	6.1	More Details
CVE-2022-33929	Dell Wyse Management Suite 3.6.1 and below contains a Reflected Cross-Site Scripting Vulnerability in EndUserSummary page. An authenticated attacker could potentially exploit this vulnerability, leading to the execution of malicious HTML or JavaScript code in a victim user's web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	6.1	More Details
CVE-2022-38358	Improper neutralization of input during web page generation leaves the Eyes of Network web application vulnerable to cross-site scripting attacks at /module/admin_notifiers/rules.php and /module/report_event/indext.php via the parameters rule_notification, rule_name, and rule_name_old, and at /module/admin_user/add_modify_user.php via the parameters user_name and user_email.	6.1	More Details
CVE-2022-36530	An issue was discovered in rageframe2 2.6.37. There is a XSS vulnerability in the user agent related parameters of the info.php page.	6.1	More Details
CVE-2022-38191	There is an HTML injection issue in Esri Portal for ArcGIS versions 10.9.0 and below which may allow a remote, authenticated attacker to inject HTML into some locations in the home application.	6.1	More Details
CVE-2022-38186	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.8.1 and below which may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the victim's browser.	6.1	More Details
CVE-2022-38193	There is a code injection vulnerability in Esri Portal for ArcGIS versions 10.8.1 and below that may allow a remote, unauthenticated attacker to pass strings which could potentially cause arbitrary code execution.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38192	A stored Cross Site Scripting (XSS) vulnerability in Esri Portal for ArcGIS may allow a remote, authenticated attacker to pass and store malicious strings via crafted queries which when accessed could potentially execute arbitrary JavaScript code in the user's browser.	6.1	More Details
CVE-2022-38188	There is a reflected XSS vulnerability in Esri Portal for ArcGIS versions 10.9.1 which may allow a remote attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the victim's browser.	6.1	More Details
CVE-2020-14320	In Moodle before 3.9.1, 3.8.4 and 3.7.7, the filter in the admin task log required extra sanitizing to prevent a reflected XSS risk.	6.1	More Details
CVE-2022-36801	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to inject arbitrary HTML or JavaScript via a Reflected Cross-Site Scripting (RXSS) vulnerability in the TeamManagement.jspa endpoint. The affected versions are before version 8.20.8.	6.1	More Details
CVE-2022-37044	In Zimbra Collaboration Suite (ZCS) 8.8.15, the URL at /h/search?action accepts parameters called extra, title, and onload that are partially sanitised and lead to reflected XSS that allows executing arbitrary JavaScript on the victim's machine.	6.1	More Details
CVE-2022-2378	The Easy Student Results WordPress plugin through 2.2.8 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-2116	The Contact Form DB WordPress plugin before 1.8.0 does not sanitise and escape some parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-2390	Apps developed with Google Play Services SDK incorrectly had the mutability flag set to PendingIntents that were passed to the Notification service. As Google Play services SDK is so widely used, this bug affects many applications. For an application affected, this bug will let the attacker, gain the access to all non-exported providers and/or gain the access to other providers the victim has permissions. We recommend upgrading to version 18.0.2 of the Play Service SDK as well as rebuilding and redeploying apps.	6.1	More Details
CVE-2022-35943	Shield is an authentication and authorization framework for CodeIgniter 4. This vulnerability may allow [SameSite Attackers](https://canitakeyoursubdomain.name/) to bypass the [CodeIgniter4 CSRF protection](https://codeigniter4.github.io/userguide/libraries/security.html) mechanism with CodeIgniter Shield. For this attack to succeed, the attacker must have direct (or indirect, e.g., XSS) control over a subdomain site (e.g., `https://a.example.com/`) of the target site (e.g., `http://example.com/`). Upgrade to **CodeIgniter v4.2.3 or later** and **Shield v1.0.0-beta.2 or later**. As a workaround: set `Config\Security::$csrfProtection` to `'session,'`remove old session data right after login (immediately after ID and password match) and regenerate CSRF token right after login (immediately after ID and password match)	5.9	More Details
CVE-2022-22983	VMware Workstation (16.x prior to 16.2.4) contains an unprotected storage of credentials vulnerability. A malicious actor with local user privileges to the victim machine may exploit this vulnerability leading to the disclosure of user passwords of the remote server connected through VMware Workstation.	5.9	More Details
CVE-2022-35956	This Rails gem adds two methods to the ActiveRecord::Base class that allow you to update many records on a single database hit, using a case sql statement for it. Before version 0.1.3 `update_by_case` gem used custom sql strings, and it was not sanitized, making it vulnerable to sql injection. Upgrade to version >= 0.1.3 that uses `Arel` instead to construct the resulting sql statement, with sanitized sql.	5.8	More Details
CVE-2022-37043	An issue was discovered in the webmail component in Zimbra Collaboration Suite (ZCS) 8.8.15 and 9.0. When using preauth, CSRF tokens are not checked on some POST endpoints. Thus, when an authenticated user views an attacker-controlled page, a request will be sent to the application that appears to be intended. The CSRF token is omitted from the request, but the request still succeeds.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46778	Execution unit scheduler contention may lead to a side channel vulnerability found on AMD CPU microarchitectures codenamed “Zen 1”, “Zen 2” and “Zen 3” that use simultaneous multithreading (SMT). By measuring the contention level on scheduler queues an attacker may potentially leak sensitive information.	5.6	More Details
CVE-2020-14379	A flaw was found in Red Hat AMQ Broker in a way that a XEE attack can be done via Broker's configuration files, leading to denial of service and information disclosure.	5.6	More Details
CVE-2022-35000	JPEGDEC commit be4843c was discovered to contain a segmentation fault via fseek at /libio/fseek.c.	5.5	More Details
CVE-2022-34999	JPEGDEC commit be4843c was discovered to contain a FPE via DecodeJPEG at /src/jpeg.inl.	5.5	More Details
CVE-2022-35002	JPEGDEC commit be4843c was discovered to contain a segmentation fault via TIFFSHORT at /src/jpeg.inl.	5.5	More Details
CVE-2022-20279	In DevicePolicyManager, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-204877302	5.5	More Details
CVE-2022-20317	In SystemUI, there is a possible way to unexpectedly enable the external speaker due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-190199063	5.5	More Details
CVE-2022-35004	JPEGDEC commit be4843c was discovered to contain a FPE via TIFFSHORT at /src/jpeg.inl.	5.5	More Details
CVE-2022-20278	In Accounts, there is a possible way to write sensitive information to the system log due to insufficient log filtering. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-205130113	5.5	More Details
CVE-2022-20277	In DevicePolicyManager, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-205145497	5.5	More Details
CVE-2022-20276	In DevicePolicyManager, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-205706731	5.5	More Details
CVE-2022-20312	In WifiP2pManager, there is a possible toobtain WiFi P2P MAC address without user consent due to missing permission check. This could lead to local information disclosure without additional execution privileges needed. User interaction is not needed forexploitationProduct: AndroidVersions: Android-13Android ID: A-192244925	5.5	More Details
CVE-2022-20275	In DevicePolicyManager, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-205836975	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29959	Emerson OpenBSI through 2022-04-29 mishandles credential storage. It is an engineering environment for the ControlWave and Bristol Babcock line of RTUs. This environment provides access control functionality through user authentication and privilege management. The credentials for various users are stored insecurely in the SecUsers.ini file by using a simple string transformation rather than a cryptographic mechanism.	5.5	More Details
CVE-2022-20263	In ActivityManager, there is a way to read process state for other users due to a missing permission check. This could lead to local information disclosure of app usage with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-217935264	5.5	More Details
CVE-2022-20272	In PermissionController, there is a possible misunderstanding about the default SMS application's permission set due to misleading text. This could lead to local information disclosure with User privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-207672568	5.5	More Details
CVE-2022-20270	In Content, there is a possible way to learn gmail account name on the device due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-209005023	5.5	More Details
CVE-2022-20322	In PackageManager, there is a possible installed package disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-187176993	5.5	More Details
CVE-2022-20304	In Content, there is a possible way to determinate the user's account due to side channel information disclosure. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-199751919	5.5	More Details
CVE-2022-20260	In the Phone app, there is a possible crash loop due to resource exhaustion. This could lead to local persistent denial of service in the Phone app with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-220865698	5.5	More Details
CVE-2022-20323	In PackageManager, there is a possible package installation disclosure due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-187176203	5.5	More Details
CVE-2022-20324	In Framework, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-187042120	5.5	More Details
CVE-2022-20326	In Telephony, there is a possible disclosure of SIM identifiers due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-185235527	5.5	More Details
CVE-2022-20259	In Telephony, there is a possible leak of ICCID and EID due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-221431393	5.5	More Details
CVE-2022-20332	In PackageManager, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-180019130	5.5	More Details
CVE-2022-20284	In Telephony, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure of phone accounts with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-231986341	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20242	In Telephony, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-231986212	5.5	More Details
CVE-2022-20300	In Content, there is a possible way to check if the given account exists on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-200956588	5.5	More Details
CVE-2022-20303	In ContentService, there is a possible way to determine if an account is on the device without GET_ACCOUNTS permission due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-200573021	5.5	More Details
CVE-2022-20301	In Content, there is a possible way to check if an account exists on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-200956614	5.5	More Details
CVE-2021-0975	In USB Manager, there is a possible way to determine whether an app is installed, without query permissions, due to side channel information disclosure. This could lead to local information disclosure of installed packages with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-180104273	5.5	More Details
CVE-2022-20287	In AppSearchManagerService, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-204082784	5.5	More Details
CVE-2022-20288	In AppSearchManagerService, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-204082360	5.5	More Details
CVE-2022-20289	In PackageInstaller, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-203683960	5.5	More Details
CVE-2022-20290	In Midi, there is a possible way to learn about private midi devices due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-203549963	5.5	More Details
CVE-2022-20291	In AppOpsService, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-203430648	5.5	More Details
CVE-2021-0735	In PackageManager, there is a possible way to get information about installed packages ignoring limitations introduced in Android 11 due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-188913056	5.5	More Details
CVE-2022-20293	In LauncherApps, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-202298672	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20294	In Content, there is a possible way to learn about an account present on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-202160705	5.5	More Details
CVE-2022-20295	In ContentService, there is a possible way to check if an account exists on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-202160584	5.5	More Details
CVE-2022-20296	In ContentService, there is a possible way to check if an account exists on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-201794303	5.5	More Details
CVE-2022-35434	jpeg-quantsmooth before commit 8879454 contained a floating point exception (FPE) via /jpeg-quantsmooth/jpegqs+0x4f5d6c.	5.5	More Details
CVE-2021-0734	In Settings, there is a possible way to determine whether an app is installed without query permissions, due to side channel information disclosure. This could lead to local information disclosure of an installed package, without proper query permissions, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-189122911	5.5	More Details
CVE-2022-35114	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via extractFrame at /readers/swf.c.	5.5	More Details
CVE-2022-35113	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via swf_DefineLosslessBitsTagToImage at /modules/swfbits.c.	5.5	More Details
CVE-2022-35111	SWFTools commit 772e55a2 was discovered to contain a stack overflow via __sanitizer::StackDepotNode::hash(__sanitizer::StackTrace const&) at /sanitizer_common/sanitizer_stackdepot.cpp.	5.5	More Details
CVE-2022-35110	SWFTools commit 772e55a2 was discovered to contain a memory leak via /lib/mem.c.	5.5	More Details
CVE-2022-35109	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via draw_stroke at /gfxpoly/stroke.c.	5.5	More Details
CVE-2022-35108	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via DCTStream::getChar() at /xpdf/Stream.cc.	5.5	More Details
CVE-2022-35107	SWFTools commit 772e55a2 was discovered to contain a stack overflow via vfprintf at /stdio-common/vfprintf.c.	5.5	More Details
CVE-2022-35106	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via FoFiTrueType::computeTableChecksum(unsigned char*, int) at /xpdf/FoFiTrueType.cc.	5.5	More Details
CVE-2022-35105	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via /bin/png2swf+0x552cea.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35104	SWFTools commit 772e55a2 was discovered to contain a heap-buffer overflow via DCTStream::reset() at /xpdf/Stream.cc.	5.5	More Details
CVE-2022-35101	SWFTools commit 772e55a2 was discovered to contain a segmentation violation via /multiarch/memset-vec-unaligned-erms.S.	5.5	More Details
CVE-2022-20298	In ContentService, there is a possible way to check if an account exists on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-201416182	5.5	More Details
CVE-2022-20299	In ContentService, there is a possible way to check if the given account exists on the device due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-201415895	5.5	More Details
CVE-2022-36141	SWFMill commit 53d7690 was discovered to contain a segmentation violation via SWF::MethodBody::write(SWF::Writer*, SWF::Context*).	5.5	More Details
CVE-2022-36140	SWFMill commit 53d7690 was discovered to contain a segmentation violation via SWF::DeclareFunction2::write(SWF::Writer*, SWF::Context*).	5.5	More Details
CVE-2022-20285	In PackageManager, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-230868108	5.5	More Details
CVE-2022-1962	Uncontrolled recursion in the Parse functions in go/parser before Go 1.17.12 and Go 1.18.4 allow an attacker to cause a panic due to stack exhaustion via deeply nested types or declarations.	5.5	More Details
CVE-2022-20355	In get of PacProxyService.java, there is a possible system service crash due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-219498290	5.5	More Details
CVE-2022-38233	XPDF commit ffaf11c was discovered to contain a segmentation violation via DCTStream::readMCURow() at /xpdf/Stream.cc.	5.5	More Details
CVE-2022-36149	tifig v0.2.2 was discovered to contain a heap-use-after-free via temInfoEntry().	5.5	More Details
CVE-2022-20350	In onCreate of NotificationAccessConfirmationActivity.java, there is a possible way to trick the victim to grant notification access to the wrong app due to improper input validation. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-228178437	5.5	More Details
CVE-2022-38235	XPDF commit ffaf11c was discovered to contain a segmentation violation via DCTStream::getChar() at /xpdf/Stream.cc.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38234	XPDF commit ffaf11c was discovered to contain a segmentation violation via Lexer::getObj(Object*) at /xpdf/Lexer.cc.	5.5	More Details
CVE-2021-29112	An out-of-bounds read vulnerability exists when parsing a specially crafted file in Esri ArcReader 10.8.1 (and earlier) which allow an unauthenticated attacker to induce an information disclosure issue in the context of the current user.	5.5	More Details
CVE-2021-29118	An out-of-bounds read vulnerability exists when parsing a specially crafted file in Esri ArcReader 10.8.1 (and earlier) which allow an unauthenticated attacker to induce an information disclosure issue in the context of the current user.	5.5	More Details
CVE-2022-20352	In addProviderRequestListener of LocationManagerService.java, there is a possible way to learn which packages request location information due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-222473855	5.5	More Details
CVE-2022-20357	In writeToParcel of SurfaceControl.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12 Android-12LAndroid ID: A-214999987	5.5	More Details
CVE-2022-20353	In onSaveRingtone of DefaultRingtonePreference.java, there is a possible inappropriate file 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-10 Android-11 Android-12 Android-12LAndroid ID: A-221041256	5.5	More Details
CVE-2022-34264	Adobe FrameMaker versions 2019 Update 8 (and earlier) and 2020 Update 4 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-36150	tifig v0.2.2 was discovered to contain a heap-buffer overflow via __asan_memmove at /asan/asan_interceptors_memintrinsics.cpp.	5.5	More Details
CVE-2022-36151	tifig v0.2.2 was discovered to contain a segmentation violation via getType() at /common/bbox.cpp.	5.5	More Details
CVE-2022-36152	tifig v0.2.2 was discovered to contain a memory leak via operator new[](unsigned long) at /asan/asan_new_delete.cpp.	5.5	More Details
CVE-2022-36153	tifig v0.2.2 was discovered to contain a segmentation violation via std::vector<unsigned int, std::allocator<unsigned int> >::size() const at /bits/stl_vector.h.	5.5	More Details
CVE-2022-36155	tifig v0.2.2 was discovered to contain a resource allocation issue via operator new(unsigned long) at asan_new_delete.cpp.	5.5	More Details
CVE-2022-37439	In Splunk Enterprise and Universal Forwarder versions in the following table, indexing a specially crafted ZIP file using the file monitoring input can result in a crash of the application. Attempts to restart the application would result in a crash and would require manually removing the malformed file.	5.5	More Details
CVE-2022-35671	Adobe Acrobat Reader versions 22.001.20169 (and earlier), 20.005.30362 (and earlier) and 17.012.30249 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35670	Adobe Acrobat Reader versions 22.001.20169 (and earlier), 20.005.30362 (and earlier) and 17.012.30249 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-38230	XPDF commit ffaf11c was discovered to contain a floating point exception (FPE) via DCTStream::decodeImage() at /xpdf/Stream.cc.	5.5	More Details
CVE-2022-2719	In ImageMagick, a crafted file could trigger an assertion failure when a call to WriteImages was made in MagickWand/operation.c, due to a NULL image list. This could potentially cause a denial of service. This was fixed in upstream ImageMagick version 7.1.0-30.	5.5	More Details
CVE-2022-35668	Adobe Acrobat Reader versions 22.001.20169 (and earlier), 20.005.30362 (and earlier) and 17.012.30249 (and earlier) are affected by an Improper Input Validation vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-34262	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-36145	SWFMill commit 53d7690 was discovered to contain a segmentation violation via SWF::Reader::getWord().	5.5	More Details
CVE-2022-34261	Adobe Illustrator versions 26.3.1 (and earlier) and 25.4.6 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-20341	In ConnectivityService, there is a possible bypass of network permissions due to a missing permission check. This could lead to local information disclosure of tethering interfaces with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-162952629	5.5	More Details
CVE-2022-35678	Adobe Acrobat Reader versions 22.001.20169 (and earlier), 20.005.30362 (and earlier) and 17.012.30249 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-36148	fdkaac commit 53fe239 was discovered to contain a floating point exception (FPE) via wav_open at /src/wav_reader.c.	5.5	More Details
CVE-2022-36146	SWFMill commit 53d7690 was discovered to contain a memory allocation issue via operator new[] (unsigned long) at asan_new_delete.cpp.	5.5	More Details
CVE-2022-2777	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.3.1.	5.4	More Details
CVE-2022-33927	Dell Wyse Management Suite 3.6.1 and below contains a Session Fixation vulnerability. A unauthenticated attacker could exploit this by taking advantage of a user with multiple active sessions in order to hijack a user's session.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2776	A vulnerability classified as problematic has been found in SourceCodester Gym Management System. Affected is an unknown function of the file delete_user.php. The manipulation of the argument delete_user leads to denial of service. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-206172.	5.4	More Details
CVE-2021-39035	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.5, 6.1.0.0 through 6.1.0.4, and 6.1.1.0 through 6.1.1.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 213965.	5.4	More Details
CVE-2022-38189	A stored Cross Site Scripting (XSS) vulnerability in Esri Portal for ArcGIS may allow a remote, authenticated attacker to pass and store malicious strings via crafted queries which when accessed could potentially execute arbitrary JavaScript code in the user's browser.	5.4	More Details
CVE-2022-24654	Authenticated stored cross-site scripting (XSS) vulnerability in "Field Server Address" field in INTELBRAS ATA 200 Firmware 74.19.10.21 allows attackers to inject JavaScript code through a crafted payload.	5.4	More Details
CVE-2022-20820	Multiple vulnerabilities in the web interface of Cisco Webex Meetings could allow a remote attacker to conduct a cross-site scripting (XSS) attack or a frame hijacking attack against a user of the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	5.4	More Details
CVE-2022-35509	An issue was discovered in EyouCMS 1.5.8. There is a Storage XSS vulnerability that can allows an attacker to execute arbitrary Web scripts or HTML by injecting a special payload via the title parameter in the foreground contribution, allowing the attacker to obtain sensitive information.	5.4	More Details
CVE-2022-20852	Multiple vulnerabilities in the web interface of Cisco Webex Meetings could allow a remote attacker to conduct a cross-site scripting (XSS) attack or a frame hijacking attack against a user of the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	5.4	More Details
CVE-2022-35697	Adobe Experience Manager Core Components version 2.20.6 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Exploitation of this issue requires a low author privilege access.	5.4	More Details
CVE-2022-38180	In JetBrains Ktor before 2.1.0 the wrong authentication provider could be selected in some cases	5.3	More Details
CVE-2022-35948	undici is an HTTP/1.1 client, written from scratch for Node.js.`=< undici@5.8.0` users are vulnerable to _CRLF Injection_ on headers when using unsanitized input as request headers, more specifically, inside the `content-type` header. Example: ``` import { request } from 'undici' const unsanitizedContentTypeInput = 'application/json\r\n\r\nGET /foo2 HTTP/1.1' await request('http://localhost:3000, { method: 'GET', headers: { 'content-type': unsanitizedContentTypeInput }, }) ``` The above snippet will perform two requests in a single `request` API call: 1) `http://localhost:3000/` 2) `http://localhost:3000/foo2` This issue was patched in Undici v5.8.1. Sanitize input when sending content-type headers using user input as a workaround.	5.3	More Details
CVE-2022-2535	The SearchWP Live Ajax Search WordPress plugin before 1.6.2 does not ensure that users making a live search are limited to published posts only, allowing unauthenticated users to make a crafted query disclosing private/draft/pending post titles along with their permalink	5.3	More Details
CVE-2022-33989	dproxy-nexgen (aka dproxy nexgen) uses a static UDP source port (selected randomly only at boot time) in upstream queries sent to DNS resolvers. This allows DNS cache poisoning because there is not enough entropy to prevent traffic injection attacks.	5.3	More Details
CVE-2022-34259	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to impact the availability of a user's minor feature. Exploitation of this issue does not require user interaction.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33993	Misinterpretation of special domain name characters in DNRD (aka Domain Name Relay Daemon) 2.20.3 leads to cache poisoning because domain names and their associated IP addresses are cached in their misinterpreted form.	5.3	More Details
CVE-2021-39086	IBM Sterling File Gateway 6.0.0.0 through 6.0.3.5, 6.1.0.0 through 6.1.0.4, and 6.1.1.0 through 6.1.1.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 215889.	5.3	More Details
CVE-2020-1755	In Moodle before 3.8.2, 3.7.5, 3.6.9 and 3.5.11, X-Forwarded-For headers could be used to spoof a user's IP, in order to bypass remote address checks.	5.3	More Details
CVE-2022-35949	undici is an HTTP/1.1 client, written from scratch for Node.js.`undici` is vulnerable to SSRF (Server-side Request Forgery) when an application takes in **user input** into the `path/pathname` option of `undici.request`. If a user specifies a URL such as `http://127.0.0.1` or `//127.0.0.1` ```js const undici = require("undici") undici.request({origin: "http://example.com", pathname: "//127.0.0.1"}) ``` Instead of processing the request as `http://example.org//127.0.0.1` (or `http://example.org/http://127.0.0.1` when `http://127.0.0.1 is used`), it actually processes the request as `http://127.0.0.1/` and sends it to `http://127.0.0.1`. If a developer passes in user input into `path` parameter of `undici.request`, it can result in an _SSRF_ as they will assume that the hostname cannot change, when in actual fact it can change because the specified path parameter is combined with the base URL. This issue was fixed in `undici@5.8.1`. The best workaround is to validate user input before passing it to the `undici.request` call.	5.3	More Details
CVE-2022-33991	dproxy-nexgen (aka dproxy nexgen) forwards and caches DNS queries with the CD (aka checking disabled) bit set to 1. This leads to disabling of DNSSEC protection provided by upstream resolvers.	5.3	More Details
CVE-2022-2838	In Eclipse Sphinx™ before version 0.13.1, Apache Xerces XML Parser was used without disabling processing of referenced external entities allowing the injection of arbitrary definitions which is able to access local files and expose their contents via HTTP requests.	5.3	More Details
CVE-2022-35954	The GitHub Actions ToolKit provides a set of packages to make creating actions easier. The `core.exportVariable` function uses a well known delimiter that attackers can use to break out of that specific variable and assign values to other arbitrary variables. Workflows that write untrusted values to the `GITHUB_ENV` file may cause the path or other environment variables to be modified without the intention of the workflow or action author. Users should upgrade to `@actions/core v1.9.1`. If you are unable to upgrade the `@actions/core` package, you can modify your action to ensure that any user input does not contain the delimiter `_GitHubActionsFileCommandDelimeter_` before calling `core.exportVariable`.	5.0	More Details
CVE-2022-20266	In Companion, there is a possible way to keep a service running with elevated importance without showing foreground service notification due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-211757348	5.0	More Details
CVE-2022-22490	IBM Robotic Process Automation 21.0.0, 21.0.1, and 21.0.2 could allow a privileged user to obtain sensitive Azure bot credential information. IBM X-Force ID: 226342.	4.9	More Details
CVE-2022-20914	A vulnerability in the External RESTful Services (ERS) API of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker to obtain sensitive information. This vulnerability is due to excessive verbosity in a specific REST API output. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to obtain sensitive information, including administrative credentials for an external authentication server. Note: To successfully exploit this vulnerability, the attacker must have valid ERS administrative credentials.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2384	The Digital Publications by Supsystic WordPress plugin before 1.7.4 does not sanitise and escape its settings, allowing high privilege users such as admin to perform cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-2152	The Duplicate Page and Post WordPress plugin before 2.8 does not sanitise and escape its settings, allowing high privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-34156	'Hulu / フールー' App for iOS versions prior to 3.0.81 improperly verifies server certificates, which may allow an attacker to eavesdrop on an encrypted communication via a man-in-the-middle attack.	4.8	More Details
CVE-2022-34258	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker with admin privileges to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	4.8	More Details
CVE-2022-35590	A cross-site scripting (XSS) issue in the ForkCMS version 5.9.3 allows remote attackers to inject JavaScript via the "end_date" Parameter	4.8	More Details
CVE-2021-42751	A cross-site scripting (XSS) vulnerability in Rule Engine in ThingsBoard 3.3.1 allows remote attackers (with administrative access) to inject arbitrary JavaScript within the description of a rule node.	4.8	More Details
CVE-2022-35585	A stored cross-site scripting (XSS) issue in the ForkCMS version 5.9.3 allows remote attackers to inject JavaScript via the "start_date" Parameter	4.8	More Details
CVE-2022-35587	A cross-site scripting (XSS) issue in the Fork version 5.9.3 allows remote attackers to inject JavaScript via the "publish_on_date" Parameter	4.8	More Details
CVE-2022-35589	A cross-site scripting (XSS) issue in the Fork version 5.9.3 allows remote attackers to inject JavaScript via the "publish_on_time" Parameter.	4.8	More Details
CVE-2021-42750	A cross-site scripting (XSS) vulnerability in Rule Engine in ThingsBoard 3.3.1 allows remote attackers (with administrative access) to inject arbitrary JavaScript within the title of a rule node.	4.8	More Details
CVE-2022-38179	JetBrains Ktor before 2.1.0 was vulnerable to the Reflect File Download attack	4.7	More Details
CVE-2022-2749	A vulnerability was found in SourceCodester Gym Management System. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /mygym/admin/index.php?view_exercises. The manipulation leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-206017 was assigned to this vulnerability.	4.7	More Details
CVE-2022-20265	In Settings, there is a possible way to bypass factory reset permissions due to a permissions bypass. This could lead to local escalation of privilege with physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-212804898	4.6	More Details
CVE-2020-10710	A flaw was found where the Plaintext Candlepin password is disclosed while updating Red Hat Satellite through the satellite-installer. This flaw allows an attacker with sufficiently high privileges, such as root, to retrieve the Candlepin plaintext password.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20243	In Core Utilities, there is a possible log information disclosure. This could lead to local information disclosure of sensitive browsing data with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-190199986	4.4	More Details
CVE-2022-20255	In SettingsProvider, there is a possible way to read or change the default ringtone 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.Product: AndroidVersions: Android-13Android ID: A-222687217	4.4	More Details
CVE-2022-2611	Inappropriate implementation in Fullscreen API in Google Chrome on Android prior to 104.0.5112.79 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	4.3	More Details
CVE-2022-33924	Dell Wyse Management Suite 3.6.1 and below contains an Improper Access control vulnerability with which an attacker with no access to create rules could potentially exploit this vulnerability and create rules.	4.3	More Details
CVE-2022-2846	The Calendar Event Multi View WordPress plugin before 1.4.07 does not have any authorisation and CSRF checks in place when creating an event, and is also lacking sanitisation as well as escaping in some of the event fields. This could allow unauthenticated attackers to create arbitrary events and put Cross-Site Scripting payloads in it.	4.3	More Details
CVE-2022-28881	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Atlant whereby the aerdl.dll component used in certain WithSecure products unpacker function crashes which leads to scanning engine crash. The exploit can be triggered remotely by an attacker.	4.3	More Details
CVE-2022-2800	A vulnerability, which was classified as problematic, has been found in SourceCodester Gym Management System. Affected by this issue is some unknown functionality. The manipulation leads to clickjacking. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-206246 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-20713	A vulnerability in the VPN web client services component of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct browser-based attacks against users of an affected device. This vulnerability is due to improper validation of input that is passed to the VPN web client services component before being returned to the browser that is in use. An attacker could exploit this vulnerability by persuading a user to visit a website that is designed to pass malicious requests to a device that is running Cisco ASA Software or Cisco FTD Software and has web services endpoints supporting VPN features enabled. A successful exploit could allow the attacker to reflect malicious input from the affected device to the browser that is in use and conduct browser-based attacks, including cross-site scripting attacks. The attacker could not directly impact the affected device.	4.3	More Details
CVE-2022-2813	A vulnerability, which was classified as problematic, was found in SourceCodester Guest Management System. Affected is an unknown function. The manipulation leads to cleartext storage of passwords in the database. The identifier of this vulnerability is VDB-206400.	4.3	More Details
CVE-2022-31674	VMware vRealize Operations contains an information disclosure vulnerability. A low-privileged malicious actor with network access can access log files that lead to information disclosure.	4.3	More Details
CVE-2022-33930	Dell Wyse Management Suite 3.6.1 and below contains Information Disclosure in Devices error pages. An attacker could potentially exploit this vulnerability, leading to the disclosure of certain sensitive information. The attacker may be able to use the exposed information to access and further vulnerability research.	4.3	More Details
CVE-2022-2619	Insufficient validation of untrusted input in Settings in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted HTML page.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2814	A vulnerability has been found in SourceCodester Simple and Nice Shopping Cart Script and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /mkshope/login.php. The manipulation of the argument msg leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-206401 was assigned to this vulnerability.	3.5	More Details
CVE-2022-2773	A vulnerability was found in SourceCodester Apartment Visitor Management System. It has been classified as problematic. This affects an unknown part of the file profile.php. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-206169 was assigned to this vulnerability.	3.5	More Details
CVE-2022-2748	A vulnerability was found in SourceCodester Simple Online Book Store System. It has been classified as problematic. Affected is an unknown function of the file /admin/edit.php. The manipulation of the argument eid leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-206016.	3.5	More Details
CVE-2022-2843	A vulnerability was found in MotoPress Timetable and Event Schedule. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /wp-admin/admin-ajax.php of the component Quick Edit. The manipulation of the argument post_title with the input <img src=x onerror=alert`2`> leads to cross site scripting. The attack may be launched remotely. VDB-206486 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-2844	A vulnerability classified as problematic has been found in MotoPress Timetable and Event Schedule up to 1.4.06. This affects an unknown part of the file /wp/?cpmvc_id=1&cpmvc_do_action=mvparse&f=datafeed&calid=1&month_index=1&method=adddetails&id=2 of the component Calendar Handler. The manipulation of the argument Subject/Location/Description leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-206487.	3.5	More Details
CVE-2022-2769	A vulnerability, which was classified as problematic, has been found in SourceCodester Company Website CMS. This issue affects some unknown processing of the file /dashboard/contact. The manipulation of the argument phone leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-206165 was assigned to this vulnerability.	3.5	More Details
CVE-2022-2768	A vulnerability classified as problematic was found in SourceCodester Library Management System. This vulnerability affects unknown code of the file /qr/l/. The manipulation of the argument error leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-206164.	3.5	More Details
CVE-2022-2767	A vulnerability classified as problematic has been found in SourceCodester Online Admission System. This affects an unknown part of the file /index.php. The manipulation of the argument student_add leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-206163.	3.5	More Details
CVE-2022-20330	In Bluetooth, there is a possible way to connect or disconnect bluetooth devices without user awareness 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-13Android ID: A-181962588	3.5	More Details
CVE-2022-35932	Nextcloud Talk is a video and audio conferencing app for Nextcloud. Prior to versions 12.2.7, 13.0.7, and 14.0.3, password protected conversations are susceptible to brute force attacks if the attacker has the link/conversation token. It is recommended that the Nextcloud Talk application is upgraded to 12.2.7, 13.0.7 or 14.0.3. There are currently no known workarounds available apart from not having password protected conversations.	3.5	More Details
CVE-2022-2811	A vulnerability classified as problematic has been found in SourceCodester Guest Management System. This affects an unknown part of the file myform.php. The manipulation of the argument name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-206397 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20251	In LocaleManager, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-225881167	3.3	More Details
CVE-2022-20249	In LocaleManager, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-226900861	3.3	More Details
CVE-2022-20252	In PackageManager, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-224547584	3.3	More Details
CVE-2022-20342	In WiFi, there is a possible disclosure of WiFi password to the end user due to an insecure default value. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-143534321	3.3	More Details
CVE-2022-20305	In ContentService, there is a possible disclosure of available account types due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-199751623	3.3	More Details
CVE-2022-20339	In Android, there is a possible access of network neighbor table information due to an insecure SEpolicy configuration. This could lead to local information disclosure of network topography with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-171572148	3.3	More Details
CVE-2022-20358	In startSync of AbstractThreadedSyncAdapter.java, there is a possible way to access protected content of content providers due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-203229608	3.3	More Details
CVE-2022-20338	In HierarchicalUri.readFrom of Uri.java, there is a possible way to craft a malformed Uri object due to improper input validation. This could lead to a local escalation of privilege, preventing processes from validating URIs correctly, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-171966843	3.3	More Details
CVE-2022-20336	In Settings, there is a possible installed application disclosure due to a missing permission check. This could lead to local information disclosure of applications allow-listed to use the network during VPN lockdown mode with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-177239688	3.3	More Details
CVE-2022-20335	In Wifi Slice, there is a possible way to adjust Wi-Fi settings even when the permission has been disabled 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.Product: AndroidVersions: Android-13Android ID: A-178014725	3.3	More Details
CVE-2022-20241	In Messaging, there is a possible way to attach a private file to an SMS message 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-13Android ID: A-217185011	3.3	More Details
CVE-2022-20340	In SELinux policy, there is a possible way of inferring which websites are being opened in the browser due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-166269532	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20328	In PackageManager, there is a possible way to determine whether an app is installed due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-184948501	3.3	More Details
CVE-2022-20318	In PackageInstaller, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-194694069	3.3	More Details
CVE-2022-20280	In MMSProvider, there is a possible read of protected data due to improper input validationSQL injection. This could lead to local information disclosure of sms/mms data with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-204117261	3.3	More Details
CVE-2022-20307	In AlarmManagerService, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-198782887	3.3	More Details
CVE-2022-20309	In PackageInstaller, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-194694094	3.3	More Details
CVE-2022-20310	In Telecomm, there is a possible disclosure of registered self managed phone accounts due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-192663798	3.3	More Details
CVE-2022-20257	In Bluetooth, there is a possible way to pair a display only device without PIN confirmation due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-222289114	3.3	More Details
CVE-2022-20311	In Telecomm, there is a possible disclosure of registered self managed phone accounts due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-192663553	3.3	More Details
CVE-2022-20316	In ContentResolver, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-190726121	3.3	More Details
CVE-2022-20315	In ActivityManager, there is a possible disclosure of installed packages due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-191058227	3.3	More Details
CVE-2022-20262	In ActivityManager, there is a possible way to check another process's capabilities due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-218338453	3.3	More Details
CVE-2022-20321	In Settings, there is a possible way for an application without permissions to read content of WiFi QR codes due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-187176859	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20267	In bluetooth, there is a possible way to enable or disable bluetooth connection without user consent 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-13Android ID: A-211646835	3.3	More Details
CVE-2022-20320	In ActivityManager, there is a possible way to determine whether an app is installed, without query permissions, 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-13Android ID: A-187956596	3.3	More Details
CVE-2022-38133	In JetBrains TeamCity before 2022.04.3 the private SSH key could be written to the server log in some cases	3.2	More Details
CVE-2022-30629	Non-random values for ticket_age_add in session tickets in crypto/tls before Go 1.17.11 and Go 1.18.3 allow an attacker that can observe TLS handshakes to correlate successive connections by comparing ticket ages during session resumption.	3.1	More Details
CVE-2022-20327	In Wi-Fi, there is a possible way to retrieve the WiFi SSID without location permissions due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-185126813	2.8	More Details
CVE-2022-37438	In Splunk Enterprise versions in the following table, an authenticated user can craft a dashboard that could potentially leak information (for example, username, email, and real name) about Splunk users, when visited by another user through the drilldown component. The vulnerability requires user access to create and share dashboards using Splunk Web.	2.6	More Details
CVE-2022-20245	In WindowManager, there is a possible method to create a recording of the lock screen due to an insecure default value. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-215005011	2.4	More Details
CVE-2022-20261	In LocationManager, there is a possible way to get location information due to a missing permission check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-219835125	2.3	More Details
CVE-2022-37446	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-37444	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-37443	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-37447	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-37442	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-37441	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37440	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2021-33236	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-34033. Reason: This candidate is a duplicate of CVE-2022-34033. Notes: All CVE users should reference CVE-2022-34033 instead of this candidate.	N/A	More Details
CVE-2021-33235	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-34035. Reason: This candidate is a duplicate of CVE-2022-34035. Notes: All CVE users should reference CVE-2022-34035 instead of this candidate.	N/A	More Details
CVE-2022-20359	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2022-37448	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-35958	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-37458. Reason: This candidate is a reservation duplicate of CVE-2022-37458. Notes: All CVE users should reference CVE-2022-37458 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-37449	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details
CVE-2022-20374	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2022-37445	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none	N/A	More Details