SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 21 December 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-2022-32573	A directory traversal vulnerability exists in the AssetActions.aspx addDoc functionality of Lansweeper lansweeper 10.1.1.0. A specially-crafted HTTP request can lead to arbitrary file upload. An attacker can send an HTTP request to trigger this vulnerability.	9.9	More Details
CVE-2022-44588	Unauth. SQL Injection vulnerability in Cryptocurrency Widgets Pack Plugin <=1.8.1 on WordPress.	9.9	More Details
CVE-2022-29517	A directory traversal vulnerability exists in the HelpdeskActions.aspx edittemplate functionality of Lansweeper lansweeper 10.1.1.0. A specially-crafted HTTP request can lead to arbitrary file upload. An attacker can send an HTTP request to trigger this vulnerability.	9.9	More Details
CVE-2022-44109	pdftojson commit 94204bb was discovered to contain a stack overflow via the component Stream::makeFilter(char*, Stream*, Object*, int).	9.8	More Details
CVE-2022-4606	PHP Remote File Inclusion in GitHub repository flatpressblog/flatpress prior to 1.3.	9.8	More Details
CVE-2022-44456	CONPROSYS HMI System (CHS) Ver.3.4.4?and earlier allows a remote unauthenticated attacker to execute an arbitrary OS command on the server where the product is running by sending a specially crafted request.	9.8	More Details
CVE-2022-44750	HCL Domino is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44754. This vulnerability applies to software previously licensed by IBM.	9.8	More Details
CVE-2022-44751	HCL Notes is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44755. This vulnerability applies to software previously licensed by IBM.	9.8	More Details
CVE-2022-44752	HCL Domino is susceptible to a stack based buffer overflow vulnerability in wp6sr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted WordPerfect file. This vulnerability applies to software previously licensed by IBM.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44753	HCL Notes is susceptible to a stack based buffer overflow vulnerability in wp6sr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted WordPerfect file. This vulnerability applies to software previously licensed by IBM.	9.8	More Details
CVE-2022-44754	HCL Domino is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44750. This vulnerability applies to software previously licensed by IBM.	9.8	More Details
CVE-2022-44755	HCL Notes is susceptible to a stack based buffer overflow vulnerability in lasr.dll in Micro Focus KeyView. This could allow a remote unauthenticated attacker to crash the application or execute arbitrary code via a crafted Lotus Ami Pro file. This is different from the vulnerability described in CVE-2022-44751. This vulnerability applies to software previously licensed by IBM.	9.8	More Details
CVE-2022-4050	The JoomSport WordPress plugin before 5.2.8 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users	9.8	More Details
CVE-2022-4063	The InPost Gallery WordPress plugin before 2.1.4.1 insecurely uses PHP's extract() function when rendering HTML views, allowing attackers to force the inclusion of malicious files & URLs, which may enable them to run code on servers.	9.8	More Details
CVE-2022-40434	Softr v2.0 was discovered to be vulnerable to HTML injection via the Name field of the Account page.	9.8	More Details
CVE-2022-44108	pdftojson commit 94204bb was discovered to contain a stack overflow via the component Object::copy(Object*):Object.cc.	9.8	More Details
CVE-2021-31650	A SQL injection vulnerability in Sourcecodester Online Grading System 1.0 allows remote attackers to execute arbitrary SQL commands via the uname parameter.	9.8	More Details
CVE-2021-38241	Deserialization issue discovered in Ruoyi before 4.6.1 allows remote attackers to run arbitrary code via weak cipher in Shiro framework.	9.8	More Details
CVE-2022-46421	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache Software Foundation Apache Airflow Hive Provider.This issue affects Apache Airflow Hive Provider: before 5.0.0.	9.8	More Details
CVE-2022-40624	pfSense pfBlockerNG through 2.1.4_27 allows remote attackers to execute arbitrary OS commands as root via the HTTP Host header, a different vulnerability than CVE-2022-31814.	9.8	More Details
CVE-2022-46538	Tenda F1203 V2.0.1.6 was discovered to contain a command injection vulnerability via the mac parameter at /goform/WriteFacMac.	9.8	More Details
CVE-2022-46020	WBCE CMS v1.5.4 can implement getshell by modifying the upload file type.	9.8	More Details
CVE-2022-46316	A thread security vulnerability exists in the authentication process. Successful exploitation of this vulnerability may affect data integrity, confidentiality, and availability.	9.8	More Details
CVE-2022-46319	Fingerprint calibration has a vulnerability of lacking boundary judgment. Successful exploitation of this vulnerability may cause out-of-bounds write.	9.8	More Details
CVE-2022-46320	The kernel module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may cause memory overwriting.	9.8	More Details
CVE-2022-46323	Some smartphones have the out-of-bounds write vulnerability.Successful exploitation of this vulnerability may cause system service exceptions.	9.8	More Details
CVE-2022-46324	Some smartphones have the out-of-bounds write vulnerability. Successful exploitation of this vulnerability may cause system service exceptions.	9.8	More Details
CVE-2022-46325	Some smartphones have the out-of-bounds write vulnerability.Successful exploitation of this vulnerability may cause system service exceptions.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46326	Some smartphones have the out-of-bounds write vulnerability. Successful exploitation of this vulnerability may cause system service exceptions.	9.8	More Details
CVE-2022-46327	Some smartphones have configuration issues. Successful exploitation of this vulnerability may cause privilege escalation, which results in system service exceptions.	9.8	More Details
CVE-2022-37832	Mutiny 7.2.0-10788 suffers from Hardcoded root password.	9.8	More Details
CVE-2022-47629	Libksba before 1.6.3 is prone to an integer overflow vulnerability in the CRL signature parser.	9.8	More Details
CVE-2022-44832	D-Link DIR-3040 device with firmware 120B03 was discovered to contain a command injection vulnerability via the SetTriggerLEDBlink function.	9.8	More Details
CVE-2021-4226	RSFirewall tries to identify the original IP address by looking at different HTTP headers. A bypass is possible due to the way it is implemented.	9.8	More Details
CVE-2022-46609	Python3-RESTfulAPI commit d9907f14e9e25dcdb54f5b22252b0e9452e3970e and e772e0beee284c50946e94c54a1d43071ca78b74 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-46996	vSphere_selfuse commit 2a9fe074a64f6a0dd8ac02f21e2f10d66cac5749 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-46997	Passhunt commit 54eb987d30ead2b8ebbf1f0b880aa14249323867 was discovered to contain a code execution backdoor via the request package. This vulnerability allows attackers to access sensitive user information and digital currency keys, as well as escalate privileges.	9.8	More Details
CVE-2022-46071	There is SQL Injection vulnerability at Helmet Store Showroom v1.0 Login Page. This vulnerability can be exploited to bypass admin access.	9.8	More Details
CVE-2022-46072	Helmet Store Showroom v1.0 vulnerable to unauthenticated SQL Injection.	9.8	More Details
CVE-2022-46255	An improper limitation of a pathname to a restricted directory vulnerability was identified in GitHub Enterprise Server that enabled remote code execution. A check was added within Pages to ensure the working directory is clean before unpacking new content to prevent an arbitrary file overwrite bug. This vulnerability affected only version 3.7.0 of GitHub Enterprise Server and was fixed in version 3.7.1. This vulnerability was reported via the GitHub Bug Bounty program.	9.8	More Details
CVE-2022-31702	vRealize Network Insight (vRNI) contains a command injection vulnerability present in the vRNI REST API. A malicious actor with network access to the vRNI REST API can execute commands without authentication.	9.8	More Details
CVE-2022-38488	logrocket-oauth2-example through 2020-05-27 allows SQL injection via the /auth/register username parameter.	9.8	More Details
CVE-2021-33420	A deserialization issue discovered in inikulin replicator before 1.0.4 allows remote attackers to run arbitrary code via the fromSerializable function in TypedArray object.	9.8	More Details
CVE-2021-39426	An issue was discovered in /Upload/admin/admin_notify.php in Seacms 11.4 allows attackers to execute arbitrary php code via the notify1 parameter when the action parameter equals set.	9.8	More Details
CVE-2022-44236	Beijing Zed-3 Technologies Co.,Ltd VoIP simpliclty ASG 8.5.0.17807 (20181130-16:12) has a Weak password vulnerability.	9.8	More Details
CVE-2022-46631	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the wscDisabled parameter in the setting/setWiFiSignalCfg function.	9.8	More Details
CVE-2022-42529	Product: AndroidVersions: Android kernelAndroid ID: A-235292841References: N/A	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47377	Password recovery vulnerability in SICK SIM2000ST Partnumber 2086502 with firmware version <1.13.4 allows an unprivileged remote attacker to gain access to the userlevel defined as RecoverableUserLevel by invocating the password recovery mechanism method. This leads to an increase in their privileges on the system and thereby affecting the confidentiality integrity and availability of the system. An attacker can expect repeatable success by exploiting the vulnerability. The recommended solution is to update the firmware to a version >= 1.13.4 as soon as possible (available in SICK Support Portal).	9.8	More Details
CVE-2022-42842	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.2, macOS Monterey 12.6.2, macOS Ventura 13.1, macOS Big Sur 11.7.2, iOS 16.2 and iPadOS 16.2, watchOS 9.2. A remote user may be able to cause kernel code execution.	9.8	More Details
CVE-2022-46393	An issue was discovered in Mbed TLS before 2.28.2 and 3.x before 3.3.0. There is a potential heap-based buffer overflow and heap-based buffer over-read in DTLS if MBEDTLS_SSL_DTLS_CONNECTION_ID is enabled and MBEDTLS_SSL_CID_IN_LEN_MAX > 2 * MBEDTLS_SSL_CID_OUT_LEN_MAX.	9.8	More Details
CVE-2022-45969	Alist v3.4.0 is vulnerable to Directory Traversal,	9.8	More Details
CVE-2022-46634	TOTOlink A7100RU V7.4cu.2313_B20191024 was discovered to contain a command injection vulnerability via the wscDisabled parameter in the setting/setWiFiWpsCfg function.	9.8	More Details
CVE-2022-42837	An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1, iOS 15.7.2 and iPadOS 15.7.2, watchOS 9.2. A remote user may be able to cause unexpected app termination or arbitrary code execution.	9.8	More Details
CVE-2022-40004	Cross Site Scripting (XSS) vulnerability in Things Board 3.4.1 allows remote attackers to escalate privilege via crafted URL to the Audit Log.	9.6	More Details
CVE-2022-28173	The web server of some Hikvision wireless bridge products have an access control vulnerability which can be used to obtain the admin permission. The attacker can exploit the vulnerability by sending crafted messages to the affected devices.	9.1	More Details
CVE-2022-47408	An issue was discovered in the fp_newsletter (aka Newsletter subscriber management) extension before 1.1.1, 1.2.0, 2.x before 2.1.2, 2.2.1 through 2.4.0, and 3.x before 3.2.6 for TYPO3. There is a CAPTCHA bypass that can lead to subscribing many people.	9.1	More Details
CVE-2022-47409	An issue was discovered in the fp_newsletter (aka Newsletter subscriber management) extension before 1.1.1, 1.2.0, 2.x before 2.1.2, 2.2.1 through 2.4.0, and 3.x before 3.2.6 for TYPO3. Attackers can unsubscribe everyone via a series of modified subscription UIDs in deleteAction operations.	9.1	More Details
CVE-2022-47410	An issue was discovered in the fp_newsletter (aka Newsletter subscriber management) extension before 1.1.1, 1.2.0, 2.x before 2.1.2, 2.2.1 through 2.4.0, and 3.x before 3.2.6 for TYPO3. Data about subscribers may be obtained via createAction operations.	9.1	More Details
CVE-2022-47411	An issue was discovered in the fp_newsletter (aka Newsletter subscriber management) extension before 1.1.1, 1.2.0, 2.x before 2.1.2, 2.2.1 through 2.4.0, and 3.x before 3.2.6 for TYPO3. Data about subscribers may be obtained via unsubscribeAction operations.	9.1	More Details
CVE-2022-45796	Command injection vulnerability in nw_interface.html in SHARP multifunction printers (MFPs)'s Digital Full-color Multifunctional System 202 or earlier, 120 or earlier, 600 or earlier, 121 or earlier, 500 or earlier, 402 or earlier, 790 or earlier, and Digital Multifunctional System (Monochrome) 200 or earlier, 211 or earlier, 102 or earlier, 453 or earlier, 400 or earlier, 202 or earlier, 602 or earlier, 500 or earlier, 401 or earlier allows remote attackers to execute arbitrary commands via unspecified vectors.	9.1	More Details
CVE-2022-44940	Patchelf v0.9 was discovered to contain an out-of-bounds read via the function modifyRPath at src/patchelf.cc.	9.1	More Details
CVE-2022-31358	A reflected cross-site scripting (XSS) vulnerability in Proxmox Virtual Environment prior to v7.2-3 allows remote attackers to execute arbitrary web scripts or HTML via non-existent endpoints under path /api2/html/.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-37155	RCE in SPIP 3.1.13 through 4.1.2 allows remote authenticated users to execute arbitrary code via the _oups parameter.	8.8	More Details
CVE-2022-47514	An XML external entity (XXE) injection vulnerability in XML-RPC.NET before 2.5.0 allows remote authenticated users to conduct server-side request forgery (SSRF) attacks, as demonstrated by a pingback.aspx POST request.	8.8	More Details
CVE-2022-46074	Helmet Store Showroom 1.0 is vulnerable to Cross Site Request Forgery (CSRF). An unauthenticated user can add an admin account due to missing CSRF protection.	8.8	More Details
CVE-2022-46341	A vulnerability was found in X.Org. This security flaw occurs because the handler for the XIPassiveUngrab request accesses out-of-bounds memory when invoked with a high keycode or button code. This issue can lead to local privileges elevation on systems where the X server is running privileged and remote code execution for ssh X forwarding sessions.	8.8	More Details
CVE-2022-42856	A type confusion issue was addressed with improved state handling. This issue is fixed in Safari 16.2, tvOS 16.2, macOS Ventura 13.1, iOS 15.7.2 and iPadOS 15.7.2, iOS 16.1.2. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.1..	8.8	More Details
CVE-2022-42861	This issue was addressed with improved checks. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Monterey 12.6.2, macOS Ventura 13.1, iOS 15.7.2 and iPadOS 15.7.2. An app may be able to break out of its sandbox.	8.8	More Details
CVE-2020-20588	File upload vulnerability in function upload in action/Core.class.php in zhimengzhe iBarn 1.5 allows remote attackers to run arbitrary code via avatar upload to index.php.	8.8	More Details
CVE-2022-25628	An authenticated user can perform XML eXternal Entity injection in Management Console in Symantec Identity Manager 14.4	8.8	More Details
CVE-2022-20610	In cellular modem firmware, there is a possible out of bounds read due to a missing bounds check. This could lead to remote code execution with LTE authentication needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-240462530References: N/A	8.8	More Details
CVE-2022-20607	In the Pixel cellular firmware, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with LTE authentication needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238914868References: N/A	8.8	More Details
CVE-2022-42863	A memory corruption issue was addressed with improved state management. This issue is fixed in Safari 16.2, tvOS 16.2, macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2, watchOS 9.2. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-42867	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 16.2, tvOS 16.2, macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2, watchOS 9.2. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-46691	A memory consumption issue was addressed with improved memory handling. This issue is fixed in Safari 16.2, tvOS 16.2, macOS Ventura 13.1, iOS 15.7.2 and iPadOS 15.7.2, iOS 16.2 and iPadOS 16.2, watchOS 9.2. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-46256	A path traversal vulnerability was identified in GitHub Enterprise Server that allowed remote code execution when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the instance. This vulnerability was fixed in versions 3.3.17, 3.4.12, 3.5.9, 3.6.5 and 3.7.2. This vulnerability was reported via the GitHub Bug Bounty program.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46443	mesinkasir Bangresto 1.0 is vulnberable to SQL Injection via the itemqty%5B%5D parameter.	8.8	More Details
CVE-2022-4506	Unrestricted Upload of File with Dangerous Type in GitHub repository openemr/openemr prior to 7.0.0.2.	8.8	More Details
CVE-2022-4505	Authorization Bypass Through User-Controlled Key in GitHub repository openemr/openemr prior to 7.0.0.2.	8.8	More Details
CVE-2022-46696	A memory corruption issue was addressed with improved input validation. This issue is fixed in Safari 16.2, tvOS 16.2, macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2, watchOS 9.2. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-46699	A memory corruption issue was addressed with improved state management. This issue is fixed in Safari 16.2, tvOS 16.2, macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2, watchOS 9.2. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-46700	A memory corruption issue was addressed with improved input validation. This issue is fixed in Safari 16.2, tvOS 16.2, macOS Ventura 13.1, iOS 15.7.2 and iPadOS 15.7.2, iOS 16.2 and iPadOS 16.2, watchOS 9.2. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-46344	A vulnerability was found in X.Org. This security flaw occurs because the handler for the XIChangeProperty request has a length-validation issues, resulting in out-of-bounds memory reads and potential information disclosure. This issue can lead to local privileges elevation on systems where the X server is running privileged and remote code execution for ssh X forwarding sessions.	8.8	More Details
CVE-2022-46343	A vulnerability was found in X.Org. This security flaw occurs because the handler for the ScreenSaverSetAttributes request may write to memory after it has been freed. This issue can lead to local privileges elevation on systems where the X server is running privileged and remote code execution for ssh X forwarding sessions.	8.8	More Details
CVE-2022-46342	A vulnerability was found in X.Org. This security flaw occurs because the handler for the XvdiSelectVideoNotify request may write to memory after it has been freed. This issue can lead to local privileges elevation on systems where the X se	8.8	More Details
CVE-2022-47209	A support user exists on the device and appears to be a backdoor for Technical Support staff. The default password for this account is “support” and cannot be changed by a user via any normally accessible means.	8.8	More Details
CVE-2022-47208	The “puhttpsniff” service, which runs by default, is susceptible to command injection due to improperly sanitized user input. An unauthenticated attacker on the same network segment as the router can execute arbitrary commands on the device without authentication.	8.8	More Details
CVE-2022-4440	Use after free in Profiles in Google Chrome prior to 108.0.5359.124 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2022-34271	A vulnerability in import module of Apache Atlas allows an authenticated user to write to web server filesystem. This issue affects Apache Atlas versions from 0.8.4 to 2.2.0.	8.8	More Details
CVE-2022-42139	Delta Electronics DVW-W02W2-E2 1.5.0.10 is vulnerable to Command Injection via Crafted URL.	8.8	More Details
CVE-2022-46914	An issue in the firmware update process of TP-LINK TL-WA801N / TL-WA801ND V1 v3.12.16 and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46912	An issue in the firmware update process of TP-Link TL-WR841N / TL-WA841ND V7 3.13.9 and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image.	8.8	More Details
CVE-2022-46910	An issue in the firmware update process of TP-Link TL-WA901ND V1 up to v3.11.2 and TL-WA901N V2 up to v3.12.16 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image.	8.8	More Details
CVE-2022-46435	An issue in the firmware update process of TP-Link TL-WR941ND V2/V3 up to 3.13.9 and TL-WR941ND V4 up to 3.12.8 allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image.	8.8	More Details
CVE-2022-4436	Use after free in Blink Media in Google Chrome prior to 108.0.5359.124 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-4437	Use after free in Mojo IPC in Google Chrome prior to 108.0.5359.124 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-4438	Use after free in Blink Frames in Google Chrome prior to 108.0.5359.124 allowed a remote attacker who convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-4439	Use after free in Aura in Google Chrome on Windows prior to 108.0.5359.124 allowed a remote attacker who convinced the user to engage in specific UI interactions to potentially exploit heap corruption via specific UI interactions. (Chromium security severity: High)	8.8	More Details
CVE-2022-45942	A Remote Code Execution (RCE) vulnerability was found in includes/baijiacms/common.inc.php in baijiacms v4.	8.8	More Details
CVE-2022-46340	A vulnerability was found in X.Org. This security flaw occurs becuase the swap handler for the XTestFakeInput request of the XTest extension may corrupt the stack if GenericEvents with lengths larger than 32 bytes are sent through a the XTestFakeInput request. This issue can lead to local privileges elevation on systems where the X server is running privileged and remote code execution for ssh X forwarding sessions. This issue does not affect systems where client and server use the same byte order.	8.8	More Details
CVE-2022-3427	The Corner Ad plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.56. This is due to missing or incorrect nonce validation on its corner_ad_settings_page function. This makes it possible for unauthenticated attackers to trigger the deletion of ads via forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-43443	OS command injection vulnerability in Buffalo network devices allows an network-adjacent attacker to execute an arbitrary OS command if a specially crafted request is sent to the management page.	8.8	More Details
CVE-2022-3752	An unauthorized user could use a specially crafted sequence of Ethernet/IP messages, combined with heavy traffic loading to cause a denial-of-service condition in Rockwell Automation Logix controllers resulting in a major non-recoverable fault. If the target device becomes unavailable, a user would have to clear the fault and redownload the user project file to bring the device back online and continue normal operation.	8.6	More Details
CVE-2022-46403	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) mishandles reject messages.	8.6	More Details
CVE-2022-38733	OnCommand Insight versions 7.3.1 through 7.3.14 are susceptible to an authentication bypass vulnerability in the Data Warehouse component.	8.6	More Details
CVE-2022-42844	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.2 and iPadOS 16.2. An app may be able to break out of its sandbox.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3157	A vulnerability exists in the Rockwell Automation controllers that allows a malformed CIP request to cause a major non-recoverable fault (MNRF) and a denial-of-service condition (DOS).	8.6	More Details
CVE-2022-2601	A buffer overflow was found in grub_font_construct_glyph(). A malicious crafted pf2 font can lead to an overflow when calculating the max_glyph_size value, allocating a smaller than needed buffer for the glyph, this further leads to a buffer overflow and a heap based out-of-bounds write. An attacker may use this vulnerability to circumvent the secure boot mechanism.	8.6	More Details
CVE-2022-22063	Memory corruption in Core due to improper configuration in boot remapper.	8.4	More Details
CVE-2022-31705	VMware ESXi, Workstation, and Fusion contain a heap out-of-bounds write vulnerability in the USB 2.0 controller (EHCI). A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.	8.2	More Details
CVE-2022-46423	An exploitable firmware modification vulnerability was discovered on the Netgear WNR2000v1 router. An attacker can conduct a MITM (Man-in-the-Middle) attack to modify the user-uploaded firmware image and bypass the CRC check, allowing attackers to execute arbitrary code or cause a Denial of Service (DoS). This affects v1.2.3.7 and earlier.	8.1	More Details
CVE-2022-46424	An exploitable firmware modification vulnerability was discovered on the Netgear XWN5001 Powerline 500 WiFi Access Point. An attacker can conduct a MITM (Man-in-the-Middle) attack to modify the user-uploaded firmware image and bypass the CRC check, allowing attackers to execute arbitrary code or cause a Denial of Service (DoS). This affects v0.4.1.1 and earlier.	8.1	More Details
CVE-2022-4567	Improper Access Control in GitHub repository openemr/openemr prior to 7.0.0.2.	8.1	More Details
CVE-2022-46701	The issue was addressed with improved bounds checks. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1, tvOS 16.2. Connecting to a malicious NFS server may lead to arbitrary code execution with kernel privileges.	7.8	More Details
CVE-2022-20507	In onMulticastListUpdateNotificationReceived of UwbEventManager.java, there is a possible arbitrary code execution due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246649179	7.8	More Details
CVE-2022-45338	An arbitrary file upload vulnerability in the profile picture upload function of Exact Synergy Enterprise 267 before 267SP13 and Exact Synergy Enterprise 500 before 500SP6 allows attackers to execute arbitrary code via a crafted SVG file.	7.8	More Details
CVE-2022-20503	In onCreate of WifiDppConfiguratorActivity.java, there is a possible way for a guest user to add a WiFi configuration 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-224772890	7.8	More Details
CVE-2022-20506	In onCreate of WifiDialogActivity.java, there is a missing permission check. This could lead to local escalation of privilege from a guest user with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-226133034	7.8	More Details
CVE-2022-42847	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.1. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-42848	A logic issue was addressed with improved checks. This issue is fixed in iOS 16.2 and iPadOS 16.2, iOS 15.7.2 and iPadOS 15.7.2, tvOS 16.2. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46697	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.1. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-46694	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 16.2 and iPadOS 16.2, iOS 15.7.2 and iPadOS 15.7.2, tvOS 16.2, watchOS 9.2. Parsing a maliciously crafted video file may lead to kernel code execution.	7.8	More Details
CVE-2022-42840	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6.2, macOS Ventura 13.1, macOS Big Sur 11.7.2, iOS 15.7.2 and iPadOS 15.7.2, iOS 16.2 and iPadOS 16.2. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-42805	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-42849	An access issue existed with privileged API calls. This issue was addressed with additional restrictions. This issue is fixed in iOS 16.2 and iPadOS 16.2, tvOS 16.2, watchOS 9.2. A user may be able to elevate privileges.	7.8	More Details
CVE-2022-46693	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in tvOS 16.2, iCloud for Windows 14.1, macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2, watchOS 9.2. Processing a maliciously crafted file may lead to arbitrary code execution.	7.8	More Details
CVE-2022-46690	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1, tvOS 16.2, watchOS 9.2. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32948	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-42850	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.2 and iPadOS 16.2. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-42841	A type confusion issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.6.2, macOS Ventura 13.1, macOS Big Sur 11.7.2. Processing a maliciously crafted package may lead to arbitrary code execution.	7.8	More Details
CVE-2022-20582	In ppmp_unprotect_mfcfw_buf of drm_fw.c, there is a possible out of bounds write 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 kernelAndroid ID: A-233645166References: N/A	7.8	More Details
CVE-2022-20508	In onAttach of ConfigureWifiSettings.java, there is a possible way for a guest user to change WiFi settings 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-218679614	7.8	More Details
CVE-2022-26582	PAX A930 device with PayDroid_7.1.1_Virgo_V04.3.26T1_20210419 can allow an attacker to gain root access through command injection in systool client. The attacker must have shell access to the device in order to exploit this vulnerability.	7.8	More Details
CVE-2022-42531	In mmu_map_for_fw of gs_ldfw_load.c, there is a possible mitigation bypass due to Permissive Memory Allocation. 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-231500967References: N/A	7.8	More Details
CVE-2022-42534	In trusty_ffa_mem_reclaim of shared-mem-smcall.c, there is a possible privilege escalation 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 kernelAndroid ID: A-237838301References: N/A	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42544	In getView of AddAppNetworksFragment.java, there is a possible way to mislead the user about network add requests 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-13Android ID: A-224545390	7.8	More Details
CVE-2022-41992	A memory corruption vulnerability exists in the VHD File Format parsing CXSPARSE record functionality of PowerISO PowerISO 8.3. A specially-crafted file can lead to an out-of-bounds write. A victim needs to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2022-4563	A vulnerability was found in Freedom of the Press SecureDrop. It has been rated as critical. Affected by this issue is some unknown functionality of the file gpg-agent.conf. The manipulation leads to symlink following. Local access is required to approach this attack. The name of the patch is b0526a06f8ca713cce74b63e00d3730618d89691. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-215972.	7.8	More Details
CVE-2022-47210	The default console presented to users over telnet (when enabled) is restricted to a subset of commands. Commands issued at this console, however, appear to be fed directly into a system call or other similar function. This allows any authenticated user to execute arbitrary commands on the device.	7.8	More Details
CVE-2022-47518	An issue was discovered in the Linux kernel before 6.0.11. Missing validation of the number of channels in drivers/net/wireless/microchip/wilc1000/cfg80211.c in the WILC1000 wireless driver can trigger a heap-based buffer overflow when copying the list of operating channels from Wi-Fi management frames.	7.8	More Details
CVE-2022-20598	In sec_media_protect of media.c, there is a possible EoP due to an integer overflow. This could lead to local escalation of privilege of secure mode MFC Core with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242357514References: N/A	7.8	More Details
CVE-2022-47519	An issue was discovered in the Linux kernel before 6.0.11. Missing validation of IEEE80211_P2P_ATTR_OPER_CHANNEL in drivers/net/wireless/microchip/wilc1000/cfg80211.c in the WILC1000 wireless driver can trigger an out-of-bounds write when parsing the channel list attribute from Wi-Fi management frames.	7.8	More Details
CVE-2022-47521	An issue was discovered in the Linux kernel before 6.0.11. Missing validation of IEEE80211_P2P_ATTR_CHANNEL_LIST in drivers/net/wireless/microchip/wilc1000/cfg80211.c in the WILC1000 wireless driver can trigger a heap-based buffer overflow when parsing the operating channel attribute from Wi-Fi management frames.	7.8	More Details
CVE-2022-42945	DWG TrueViewTM 2023 version has a DLL Search Order Hijacking vulnerability. Successful exploitation by a malicious attacker could result in remote code execution on the target system.	7.8	More Details
CVE-2022-42947	A maliciously crafted X_B file when parsed through Autodesk Maya 2023 and 2022 can be used to write beyond the allocated buffer. This vulnerability can lead to arbitrary code execution.	7.8	More Details
CVE-2022-43289	Deark v.1.6.2 was discovered to contain a stack overflow via the do_prism_read_palette() function at /modules/atari-img.c.	7.8	More Details
CVE-2022-4515	A flaw was found in Exuberant Ctags in the way it handles the "-o" option. This option specifies the tag filename. A crafted tag filename specified in the command line or in the configuration file results in arbitrary command execution because the externalSortTags() in sort.c calls the system(3) function in an unsafe way.	7.8	More Details
CVE-2022-20600	In TBD of TBD, there is a possible out of bounds write due to memory corruption. 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-239847859References: N/A	7.8	More Details
CVE-2022-20597	In ppmpu_set of ppmpu.c, there is a possible EoP 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-243480506References: N/A	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20512	In navigateUpTo of Task.java, there is a possible way to launch an intent handler with a mismatched intent 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-13Android ID: A-238602879	7.8	More Details
CVE-2022-20550	In Multiple Locations, there is a possibility 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-242845514	7.8	More Details
CVE-2022-20520	In onCreate of various files, there is a possible tapjacking/overlay attack. This could lead to local escalation of privilege or denial of server with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-227203202	7.8	More Details
CVE-2022-20522	In getSlice of ProviderModelSlice.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-13Android ID: A-227470877	7.8	More Details
CVE-2022-20524	In compose of Vibrator.cpp, there is a possible arbitrary 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-228523213	7.8	More Details
CVE-2022-20540	In SurfaceFlinger::doDump of SurfaceFlinger.cpp, there is possible arbitrary 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-237291506	7.8	More Details
CVE-2022-20547	In multiple functions of AdapterService.java, there is a possible way to manipulate Bluetooth state 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-240301753	7.8	More Details
CVE-2022-20548	In setParameter of EqualizerEffect.cpp, there is a possible out of bounds write 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-13Android ID: A-240919398	7.8	More Details
CVE-2022-20561	In TBD of aud_hal_tunnel.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-222162870References: N/A	7.8	More Details
CVE-2022-20587	In ppmp_validate_wsm of drm_fw.c, there is a possible EoP 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 kernelAndroid ID: A-238720411References: N/A	7.8	More Details
CVE-2022-20566	In l2cap_chan_put of l2cap_core, there is a possible use after free due to improper locking. 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-165329981References: Upstream kernel	7.8	More Details
CVE-2022-20568	In (TBD) of (TBD), there is a possible way to corrupt kernel memory 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 kernelAndroid ID: A-220738351References: Upstream kernel	7.8	More Details
CVE-2022-32860	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5, macOS Big Sur 11.6.8. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-20584	In page_number of shared_mem.c, there is a possible code execution in secure world 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 kernelAndroid ID: A-238366009References: N/A	7.8	More Details
CVE-2022-20585	In valid_out_of_special_sec_dram_addr of drm_access_control.c, there is a possible EoP 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 kernelAndroid ID: A-238716781References: N/A	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20586	In valid_out_of_special_sec_dram_addr of drm_access_control.c, there is a possible EoP 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 kernelAndroid ID: A-238718854References: N/A	7.8	More Details
CVE-2022-32942	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6.2, macOS Ventura 13.1, macOS Big Sur 11.7.2. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-42046	wfshbr64.sys and wfshbr32.sys specially crafted IOCTL allows arbitrary user to perform local privilege escalation	7.8	More Details
CVE-2022-44898	The MsIo64.sys component in Asus Aura Sync through v1.07.79 does not properly validate input to IOCTL 0x80102040, 0x80102044, 0x80102050, and 0x80102054, allowing attackers to trigger a memory corruption and cause a Denial of Service (DoS) or escalate privileges via crafted IOCTL requests.	7.8	More Details
CVE-2022-4283	A vulnerability was found in X.Org. This security flaw occurs because the XkbCopyNames function left a dangling pointer to freed memory, resulting in out-of-bounds memory access on subsequent XkbGetKbdByName requests.. This issue can lead to local privileges elevation on systems where the X server is running privileged and remote code execution for ssh X forwarding sessions.	7.8	More Details
CVE-2022-44910	Binbloom 2.0 was discovered to contain a heap buffer overflow via the read_pointer function at /binbloom-master/src/helpers.c.	7.8	More Details
CVE-2022-23542	OpenFGA is an authorization/permission engine built for developers and inspired by Google Zanzibar. During an internal security assessment, it was discovered that OpenFGA version 0.3.0 is vulnerable to authorization bypass under certain conditions. This issue has been patched in version 0.3.1 and is backward compatible.	7.7	More Details
CVE-2022-23512	MeterSphere is a one-stop open source continuous testing platform. Versions prior to 2.4.1 are vulnerable to Path Injection in ApiTestCaseService::deleteBodyFiles which takes a user-controlled string id and passes it to ApiTestCaseService, which uses the user-provided value (testId) in new File(BODY_FILE_DIR + "/" + testId), being deleted later by file.delete(). By adding some camouflage parameters to the url, an attacker can target files on the server. The vulnerability has been fixed in v2.4.1.	7.7	More Details
CVE-2022-46539	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the security_5g parameter at /goform/WifiBasicSet.	7.5	More Details
CVE-2022-46532	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the deviceMac parameter at /goform/addWifiMacFilter.	7.5	More Details
CVE-2022-20516	In rw_t3t_act_handle_check_ndef_rsp of rw_t3t.cc, there is a possible out of bounds read due to an integer 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-224002331	7.5	More Details
CVE-2022-45666	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the list parameter in the formwrlSSIDset function.	7.5	More Details
CVE-2022-46530	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the mac parameter at /goform/GetParentControlInfo.	7.5	More Details
CVE-2022-42524	In sms_GetTpUdIIe of sms_PduCodec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243401445References: N/A	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46531	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the deviceId parameter at /goform/addWifiMacFilter.	7.5	More Details
CVE-2022-31703	The vRealize Log Insight contains a Directory Traversal Vulnerability. An unauthenticated, malicious actor can inject files into the operating system of an impacted appliance which can result in remote code execution.	7.5	More Details
CVE-2022-46540	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the entrys parameter at /goform/addressNat.	7.5	More Details
CVE-2022-45665	Tenda i22 V1.0.0.3(4687) was discovered to contain a buffer overflow via the funcpara1 parameter in the formSetCfm function.	7.5	More Details
CVE-2022-46533	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the limitSpeed parameter at /goform/SetClientState.	7.5	More Details
CVE-2022-46534	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the speed_dir parameter at /goform/SetSpeedWan.	7.5	More Details
CVE-2016-20018	Knex Knex.js through 2.3.0 has a limited SQL injection vulnerability that can be exploited to ignore the WHERE clause of a SQL query.	7.5	More Details
CVE-2022-46535	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the deviceId parameter at /goform/SetClientState.	7.5	More Details
CVE-2022-46536	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the limitSpeedUp parameter at /goform/SetClientState.	7.5	More Details
CVE-2022-46537	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the security parameter at /goform/WifiBasicSet.	7.5	More Details
CVE-2022-4061	The JobBoardWP WordPress plugin before 1.2.2 does not properly validate file names and types in its file upload functionalities, allowing unauthenticated users to upload arbitrary files such as PHP.	7.5	More Details
CVE-2022-3166	Rockwell Automation was made aware that the webservers of the Micrologix 1100 and 1400 controllers contain a vulnerability that may lead to a denial-of-service condition. The security vulnerability could be exploited by an attacker with network access to the affected systems by sending TCP packets to webserver and closing it abruptly which would cause a denial-of-service condition for the web server application on the device	7.5	More Details
CVE-2022-46137	AeroCMS v0.0.1 is vulnerable to Directory Traversal. The impact is: obtain sensitive information (remote). The component is: AeroCMS v0.0.1.	7.5	More Details
CVE-2022-46541	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the ssid parameter at /goform/fast_setting_wifi_set.	7.5	More Details
CVE-2022-3109	An issue was discovered in the FFmpeg package, where vp3_decode_frame in libavcodec/vp3.c lacks check of the return value of av_malloc() and will cause a null pointer dereference, impacting availability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-35252	Common encryption key appears to be used across all deployed instances of Serv-U FTP Server. Because of this an encrypted value that is exposed to an attacker can be simply recovered to plaintext.	7.5	More Details
CVE-2022-20601	Product: AndroidVersions: Android kernelAndroid ID: A-204541506References: N/A	7.5	More Details
CVE-2022-20602	Product: AndroidVersions: Android kernelAndroid ID: A-211081867References: N/A	7.5	More Details
CVE-2022-45041	SQL Injection exits in xinhu < 2.5.0	7.5	More Details
CVE-2022-20605	In SAECOMM_CopyBufferBytes of SAECOMM_Utility.c, 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 not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-231722405References: N/A	7.5	More Details
CVE-2022-46399	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) is unresponsive with ConReqTimeoutZero.	7.5	More Details
CVE-2022-23517	rails-html-sanitizer is responsible for sanitizing HTML fragments in Rails applications. Certain configurations of rails-html-sanitizer < 1.4.4 use an inefficient regular expression that is susceptible to excessive backtracking when attempting to sanitize certain SVG attributes. This may lead to a denial of service through CPU resource consumption. This issue has been patched in version 1.4.4.	7.5	More Details
CVE-2022-25904	All versions of package safe-eval are vulnerable to Prototype Pollution which allows an attacker to add or modify properties of the Object.prototype.Consolidate when using the function safeEval. This is because the function uses vm variable, leading an attacker to modify properties of the Object.prototype.	7.5	More Details
CVE-2022-23514	Loofah is a general library for manipulating and transforming HTML/XML documents and fragments, built on top of Nokogiri. Loofah < 2.19.1 contains an inefficient regular expression that is susceptible to excessive backtracking when attempting to sanitize certain SVG attributes. This may lead to a denial of service through CPU resource consumption. This issue is patched in version 2.19.1.	7.5	More Details
CVE-2022-4504	Improper Input Validation in GitHub repository openemr/openemr prior to 7.0.0.2.	7.5	More Details
CVE-2022-25931	All versions of package easy-static-server are vulnerable to Directory Traversal due to missing input sanitization and sandboxes being employed to the req.url user input that is passed to the server code.	7.5	More Details
CVE-2022-46109	Tenda AC15 V15.03.06.23 is vulnerable to Buffer Overflow via function formSetClientState.	7.5	More Details
CVE-2022-25940	All versions of package lite-server are vulnerable to Denial of Service (DoS) when an attacker sends an HTTP request and includes control characters that the decodeURI() function is unable to parse.	7.5	More Details
CVE-2022-4106	The Wholesale Market for WooCommerce WordPress plugin before 1.0.7 does not have authorisation check, as well as does not validate user input used to generate system path, allowing unauthenticated attackers to download arbitrary file from the server.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23503	TYPO3 is an open source PHP based web content management system. Versions prior to 8.7.49, 9.5.38, 10.4.33, 11.5.20, and 12.1.1 are vulnerable to Code Injection. Due to the lack of separating user-submitted data from the internal configuration in the Form Designer backend module, it is possible to inject code instructions to be processed and executed via TypoScript as PHP code. The existence of individual TypoScript instructions for a particular form item and a valid backend user account with access to the form module are needed to exploit this vulnerability. This issue is patched in versions 8.7.49 ELTS, 9.5.38 ELTS, 10.4.33, 11.5.20, 12.1.1.	7.5	More Details
CVE-2022-32749	Improper Check for Unusual or Exceptional Conditions vulnerability handling requests in Apache Traffic Server allows an attacker to crash the server under certain conditions. This issue affects Apache Traffic Server: from 8.0.0 through 9.1.3.	7.5	More Details
CVE-2022-46542	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the page parameter at /goform/addressNat.	7.5	More Details
CVE-2022-47517	An issue was discovered in the libsofia-sip fork in drachtio-server before 0.8.19. It allows remote attackers to cause a denial of service (daemon crash) via a crafted UDP message that causes a url_canonize2 heap-based buffer over-read because of an off-by-one error.	7.5	More Details
CVE-2022-46434	An issue in the firmware update process of TP-Link TL-WA7510N v1 v3.12.6 and earlier allows attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image.	7.5	More Details
CVE-2022-20545	In bindArtworkAndColors of MediaControlPanel.java, there is a possible way to crash the phone due to improper input validation. 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-239368697	7.5	More Details
CVE-2021-46856	The multi-screen collaboration module has a path traversal vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-46543	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the mitInterface parameter at /goform/addressNat.	7.5	More Details
CVE-2022-41596	The system tool has inconsistent serialization and deserialization. Successful exploitation of this vulnerability will cause unauthorized startup of components.	7.5	More Details
CVE-2022-41599	The system service has a vulnerability that causes incorrect return values. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-23516	Loofah is a general library for manipulating and transforming HTML/XML documents and fragments, built on top of Nokogiri. Loofah >= 2.2.0, < 2.19.1 uses recursion for sanitizing CDATA sections, making it susceptible to stack exhaustion and raising a SystemStackError exception. This may lead to a denial of service through CPU resource consumption. This issue is patched in version 2.19.1. Users who are unable to upgrade may be able to mitigate this vulnerability by limiting the length of the strings that are sanitized.	7.5	More Details
CVE-2022-46310	The TelephonyProvider module has a vulnerability in obtaining values.Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-46311	The contacts component has a free (undefined) provider vulnerability. Successful exploitation of this vulnerability may affect data integrity.	7.5	More Details
CVE-2022-46312	The application management module has a vulnerability in permission verification. Successful exploitation of this vulnerability causes unexpected clear of device applications.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46314	The IPC module has defects introduced in the design process. Successful exploitation of this vulnerability may affect system availability.	7.5	More Details
CVE-2022-46315	The ProfileSDK has defects introduced in the design process. Successful exploitation of this vulnerability may affect system availability.	7.5	More Details
CVE-2022-46317	The power consumption module has an out-of-bounds read vulnerability. Successful exploitation of this vulnerability may affect system availability.	7.5	More Details
CVE-2022-46321	The Wi-Fi module has a vulnerability in permission verification. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-46322	Some smartphones have the out-of-bounds write vulnerability. Successful exploitation of this vulnerability may cause system service exceptions.	7.5	More Details
CVE-2022-46328	Some smartphones have the input validation vulnerability. Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-2536	The Transposh WordPress Translation plugin for WordPress is vulnerable to unauthorized setting changes by unauthenticated users in versions up to, and including, 1.0.8.1. This is due to insufficient validation of settings on the 'tp_translation' AJAX action which makes it possible for unauthenticated attackers to bypass any restrictions and influence the data shown on the site. Please note this is a separate issue from CVE-2022-2461. Notes from the researcher: When installed Transposh comes with a set of pre-configured options, one of these is the "Who can translate" setting under the "Settings" tab. However, this option is largely ignored, if Transposh has enabled its "autotranslate" feature (it's enabled by default) and the HTTP POST parameter "sr0" is larger than 0. This is caused by a faulty validation in "wp/transposh_db.php."	7.5	More Details
CVE-2022-46432	An exploitable firmware modification vulnerability was discovered on TP-Link TL-WR743ND V1. An attacker can conduct a MITM (Man-in-the-Middle) attack to modify the user-uploaded firmware image and bypass the CRC check, allowing attackers to execute arbitrary code or cause a Denial of Service (DoS). This affects v3.12.20 and earlier.	7.5	More Details
CVE-2022-41591	The backup module has a path traversal vulnerability. Successful exploitation of this vulnerability causes unauthorized access to other system files.	7.5	More Details
CVE-2022-42527	In cd_SsParseMsg of cd_SsCodec.c, 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 kernelAndroid ID: A-244448906References: N/A	7.5	More Details
CVE-2022-47515	An issue was discovered in drachtio-server before 0.8.20. It allows remote attackers to cause a denial of service (daemon crash) via a long message in a TCP request that leads to std::length_error.	7.5	More Details
CVE-2022-46544	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the cmdinput parameter at /goform/exeCommand.	7.5	More Details
CVE-2022-46545	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the page parameter at /goform/NatStaticSetting.	7.5	More Details
CVE-2022-46546	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the entrys parameter at /goform/RouteStatic.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47516	An issue was discovered in the libsofia-sip fork in drachtio-server before 0.8.20. It allows remote attackers to cause a denial of service (daemon crash) via a crafted UDP message that leads to a failure of the libsofia-sip-ua/tport/tport.c self assertion.	7.5	More Details
CVE-2022-38873	D-Link devices DAP-2310 v2.10rc036 and earlier, DAP-2330 v1.06rc020 and earlier, DAP-2360 v2.10rc050 and earlier, DAP-2553 v3.10rc031 and earlier, DAP-2660 v1.15rc093 and earlier, DAP-2690 v3.20rc106 and earlier, DAP-2695 v1.20rc119_beta31 and earlier, DAP-3320 v1.05rc027 beta and earlier, DAP-3662 v1.05rc047 and earlier allows attackers to cause a Denial of Service (DoS) via uploading a crafted firmware after modifying the firmware header.	7.5	More Details
CVE-2022-46547	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the page parameter at /goform/VirtualSer.	7.5	More Details
CVE-2022-46548	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the page parameter at /goform/DhcpListClient.	7.5	More Details
CVE-2022-46549	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the deviceId parameter at /goform/saveParentControlInfo.	7.5	More Details
CVE-2022-46550	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the urls parameter at /goform/saveParentControlInfo.	7.5	More Details
CVE-2022-20560	Product: AndroidVersions: Android kernelAndroid ID: A-212623833References: N/A	7.5	More Details
CVE-2022-46551	Tenda F1203 V2.0.1.6 was discovered to contain a buffer overflow via the time parameter at /goform/saveParentControlInfo.	7.5	More Details
CVE-2022-46076	D-Link DIR-869 DIR869Ax_FW102B15 is vulnerable to Authentication Bypass via phpcgi.	7.5	More Details
CVE-2022-25171	The package p4 before 0.0.7 are vulnerable to Command Injection via the run() function due to improper input sanitization	7.4	More Details
CVE-2022-24377	The package cycle-import-check before 1.3.2 are vulnerable to Command Injection via the writeFileToTmpDirAndOpenIt function due to improper user-input sanitization.	7.4	More Details
CVE-2022-3875	A vulnerability classified as critical was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. This vulnerability affects unknown code of the component API. The manipulation leads to authentication bypass by assumed-immutable data. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216244.	7.3	More Details
CVE-2022-23741	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed a scoped user-to-server token to escalate to full admin/owner privileges. An attacker would require an account with admin access to install a malicious GitHub App. This vulnerability was fixed in versions 3.3.17, 3.4.12, 3.5.9, and 3.6.5. This vulnerability was reported via the GitHub Bug Bounty program.	7.2	More Details
CVE-2022-46127	Helmet Store Showroom Site v1.0 is vulnerable to SQL Injection via /hss/classes/Master.php?f=delete_product.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41418	An issue in the component BlogEngine/BlogEngine.NET/AppCode/Api/UploadController.cs of BlogEngine.NET v3.3.8.0 allows attackers to execute arbitrary code via uploading a crafted PNG file.	7.2	More Details
CVE-2022-46120	Helmet Store Showroom Site v1.0 is vulnerable to SQL Injection via /hss/admin/?page=products/view_product&id=.	7.2	More Details
CVE-2022-46119	Helmet Store Showroom Site v1.0 is vulnerable to SQL Injection via /hss/?page=categories&c=.	7.2	More Details
CVE-2022-46126	Helmet Store Showroom Site v1.0 is vulnerable to SQL Injection via /hss/admin/brands/manage_brand.php?id=.	7.2	More Details
CVE-2022-42845	The issue was addressed with improved memory handling. This issue is fixed in tvOS 16.2, macOS Monterey 12.6.2, macOS Ventura 13.1, macOS Big Sur 11.7.2, iOS 16.2 and iPadOS 16.2, watchOS 9.2. An app with root privileges may be able to execute arbitrary code with kernel privileges.	7.2	More Details
CVE-2022-42140	Delta Electronics DX-2100-L1-CN 2.42 is vulnerable to Command Injection via lform/net_diagnose.	7.2	More Details
CVE-2022-46122	Helmet Store Showroom Site v1.0 is vulnerable to SQL Injection via /hss/admin/categories/view_category.php?id=.	7.2	More Details
CVE-2022-20603	In SetDecompContextDb of RohcDeCompContextOfRbId.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-219265339References: N/A	7.2	More Details
CVE-2022-46123	Helmet Store Showroom Site v1.0 is vulnerable to SQL Injection via /hss/admin/categories/manage_category.php?id=.	7.2	More Details
CVE-2022-23519	rails-html-sanitizer is responsible for sanitizing HTML fragments in Rails applications. Prior to version 1.4.4, a possible XSS vulnerability with certain configurations of Rails::Html::Sanitizer may allow an attacker to inject content if the application developer has overridden the sanitizer's allowed tags in either of the following ways: allow both "math" and "style" elements, or allow both "svg" and "style" elements. Code is only impacted if allowed tags are being overridden. . This issue is fixed in version 1.4.4. All users overriding the allowed tags to include "math" or "svg" and "style" should either upgrade or use the following workaround immediately: Remove "style" from the overridden allowed tags, or remove "math" and "svg" from the overridden allowed tags.	7.2	More Details
CVE-2022-46125	Helmet Store Showroom Site v1.0 is vulnerable to SQL Injection via /hss/admin/?page=client/manage_client&id=.	7.2	More Details
CVE-2022-46124	Helmet Store Showroom Site v1.0 is vulnerable to SQL Injection via /hss/admin/?page=user/manage_user&id=.	7.2	More Details
CVE-2022-46117	Helmet Store Showroom Site v1.0 is vulnerable to SQL Injection via /hss/?page=view_product&id=.	7.2	More Details
CVE-2022-46118	Helmet Store Showroom Site v1.0 is vulnerable to SQL Injection via /hss/?page=product_per_brand&bid=.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46121	Helmet Store Showroom Site v1.0 is vulnerable to SQL Injection via /hss/admin/?page=products/manage_product&id=.	7.2	More Details
CVE-2022-31700	VMware Workspace ONE Access and Identity Manager contain an authenticated remote code execution vulnerability. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 7.2.	7.2	More Details
CVE-2022-31707	vRealize Operations (vROps) contains a privilege escalation vulnerability. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 7.2.	7.2	More Details
CVE-2022-46135	In AeroCms v0.0.1, there is an arbitrary file upload vulnerability at /admin/posts.php?source=edit_post , through which we can upload webshell and control the web server.	7.2	More Details
CVE-2022-46670	Rockwell Automation was made aware of a vulnerability by a security researcher from Georgia Institute of Technology that the MicroLogix 1100 and 1400 controllers contain a vulnerability that may give an attacker the ability to accomplish remote code execution. The vulnerability is an unauthenticated stored cross-site scripting vulnerability in the embedded webserver. The payload is transferred to the controller over SNMP and is rendered on the homepage of the embedded website.	7.1	More Details
CVE-2022-42946	Parsing a maliciously crafted X_B and PRT file can force Autodesk Maya 2023 and 2022 to read beyond allocated buffer. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.1	More Details
CVE-2022-47520	An issue was discovered in the Linux kernel before 6.0.11. Missing offset validation in drivers/net/wireless/microchip/wilc1000/hif.c in the WILC1000 wireless driver can trigger an out-of-bounds read when parsing a Robust Security Network (RSN) information element from a Netlink packet.	7.1	More Details
CVE-2022-42855	A logic issue was addressed with improved state management. This issue is fixed in tvOS 16.2, macOS Monterey 12.6.2, macOS Ventura 13.1, iOS 15.7.2 and iPadOS 15.7.2, iOS 16.2 and iPadOS 16.2. An app may be able to use arbitrary entitlements.	7.1	More Details
CVE-2022-4501	The Mega Addons plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the vc_saving_data function in versions up to, and including, 4.2.7. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to update the plugin's settings.	7.1	More Details
CVE-2022-3775	When rendering certain unicode sequences, grub2's font code doesn't proper validate if the informed glyph's width and height is constrained within bitmap size. As consequence an attacker can craft an input which will lead to a out-of-bounds write into grub2's heap, leading to memory corruption and availability issues. Although complex, arbitrary code execution could not be discarded.	7.1	More Details
CVE-2022-47578	An issue was discovered in the endpoint protection agent in Zoho ManageEngine Device Control Plus 10.1.2228.15. Despite configuring complete restrictions on USB pendrives, USB HDD devices, memory cards, USB connections to mobile devices, etc., it is still possible to bypass the USB restrictions by booting into Safe Mode. This allows a file to be exchanged outside the laptop/system. Safe Mode can be launched by any user (even without admin rights). Data exfiltration can occur, and also malware might be introduced onto the system. NOTE: the vendor's position is "it's not a vulnerability in our product."	7.1	More Details
CVE-2022-47577	An issue was discovered in the endpoint protection agent in Zoho ManageEngine Device Control Plus 10.1.2228.15. Despite configuring complete restrictions on USB pendrives, USB HDD devices, memory cards, USB connections to mobile devices, etc., it is still possible to bypass the USB restrictions by making use of a virtual machine (VM). This allows a file to be exchanged outside the laptop/system. VMs can be created by any user (even without admin rights). The data exfiltration can occur without any record in the audit trail of Windows events on the host machine. NOTE: the vendor's position is "it's not a vulnerability in our product."	7.1	More Details
CVE-2022-42864	A race condition was addressed with improved state handling. This issue is fixed in tvOS 16.2, macOS Monterey 12.6.2, macOS Ventura 13.1, macOS Big Sur 11.7.2, iOS 15.7.2 and iPadOS 15.7.2, iOS 16.2 and iPadOS 16.2, watchOS 9.2. An app may be able to execute arbitrary code with kernel privileges.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46689	A race condition was addressed with additional validation. This issue is fixed in tvOS 16.2, macOS Monterey 12.6.2, macOS Ventura 13.1, macOS Big Sur 11.7.2, iOS 15.7.2 and iPadOS 15.7.2, iOS 16.2 and iPadOS 16.2, watchOS 9.2. An app may be able to execute arbitrary code with kernel privileges.	7.0	More Details
CVE-2022-42453	There are insufficient warnings when a Fixlet is imported by a user. The warning message currently assumes the owner of the script is the logged in user, with insufficient warnings when attempting to run the script.	6.9	More Details
CVE-2022-26581	PAX A930 device with PayDroid_7.1.1_Virgo_V04.3.26T1_20210419 can allow an unauthorized attacker to perform privileged actions through the execution of specific binaries listed in ADB daemon. The attacker must have physical USB access to the device in order to exploit this vulnerability.	6.8	More Details
CVE-2020-4497	IBM Spectrum Protect Plus 10.1.0 through 10.1.12 discloses sensitive information due to unencrypted data being used in the communication flow between Spectrum Protect Plus vSnap and its agents. An attacker could obtain information using main in the middle techniques. IBM X-Force ID: 182106.	6.8	More Details
CVE-2022-40607	IBM Spectrum Scale 5.1 could allow users with permissions to create pod, persistent volume and persistent volume claim to access files and directories outside of the volume, including on the host filesystem. IBM X-Force ID: 235740.	6.8	More Details
CVE-2022-26580	PAX A930 device with PayDroid_7.1.1_Virgo_V04.3.26T1_20210419 can allow the execution of specific command injections on selected binaries in the ADB daemon shell service. The attacker must have physical USB access to the device in order to exploit this vulnerability.	6.8	More Details
CVE-2022-43466	OS command injection vulnerability in Buffalo network devices allows a network-adjacent attacker with an administrative privilege to execute an arbitrary OS command if a specially crafted request is sent to a specific CGI program.	6.8	More Details
CVE-2022-43486	Hidden functionality vulnerability in Buffalo network devices allows a network-adjacent attacker with an administrative privilege to enable the debug functionalities and execute an arbitrary command on the affected devices.	6.8	More Details
CVE-2022-42508	In ProtocolCallBuilder::BuildSendUssd of protocolcallbuilder.cpp, 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 kernelAndroid ID: A-241388966References: N/A	6.7	More Details
CVE-2022-42505	In ProtocolMiscBuilder::BuildSetSignalReportCriteria of protocolmiscbuilder.cpp, 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 kernelAndroid ID: A-241232492References: N/A	6.7	More Details
CVE-2022-20564	In _ufdt_output_strtab_to_fdt of ufdt_convert.c, 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 kernelAndroid ID: A-243798789References: N/A	6.7	More Details
CVE-2022-20563	In TBD of ufdt_convert, there is a possible out of bounds read due to memory corruption. 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-242067561References: N/A	6.7	More Details
CVE-2022-20554	In removeEventHubDevice of InputDevice.cpp, there is a possible OOB read 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-245770596	6.7	More Details
CVE-2022-42506	In SimUpdatePbEntry::encode of simdata.cpp, 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 kernelAndroid ID: A-241388399References: N/A	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42507	In ProtocolSimBuilder::BuildSimUpdatePb3gEntry of protocolsimbuilder.cpp, 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 kernelAndroid ID: A-241388774References: N/A	6.7	More Details
CVE-2022-42509	In CallDialReqData::encode of callreqdata.cpp, 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 kernelAndroid ID: A-241544307References: N/A	6.7	More Details
CVE-2022-42510	In StringsRequestData::encode of requestdata.cpp, there is a possible out of bounds read 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-241762656References: N/A	6.7	More Details
CVE-2022-42504	In CallDialReqData::encodeCallNumber of callreqdata.cpp, 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 kernelAndroid ID: A-241232209References: N/A	6.7	More Details
CVE-2022-42511	In EmbmsSessionData::encode of embmsdata.cpp, 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 kernelAndroid ID: A-241762712References: N/A	6.7	More Details
CVE-2022-42513	In ProtocolEmbmsBuilder::BuildSetSession of protocolembmsbuilder.cpp, 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 kernelAndroid ID: A-241763204References: N/A	6.7	More Details
CVE-2022-20557	In MessageQueueBase of MessageQueueBase.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-247092734	6.7	More Details
CVE-2022-42520	In ServiceInterface::HandleRequest of serviceinterface.cpp, there is a possible 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-242994270References: N/A	6.7	More Details
CVE-2022-42521	In encode of wlandata.cpp, 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-243130019References: N/A	6.7	More Details
CVE-2022-20596	In sendChunk of WirelessCharger.cpp, 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 kernelAndroid ID: A-239700400References: N/A	6.7	More Details
CVE-2022-42502	In FacilityLock::Parse of simdata.cpp, 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 kernelAndroid ID: A-241231970References: N/A	6.7	More Details
CVE-2022-20569	In thermal_cooling_device_stats_update of thermal_sysfs.c, there is a possible out of bounds write due to improper input validation. 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-229258234References: N/A	6.7	More Details
CVE-2022-42503	In ProtocolMiscBuilder::BuildSetLinkCapaReportCriteria of protocolmiscbuilder.cpp, 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 kernelAndroid ID: A-241231983References: N/A	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20594	In updateStart of WirelessCharger.cpp, 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 kernelAndroid ID: A-239567689References: N/A	6.7	More Details
CVE-2022-20599	In Pixel firmware, there is a possible exposure of sensitive memory 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 kernelAndroid ID: A-242332706References: N/A	6.7	More Details
CVE-2022-20588	In sysmmu_map of sysmmu.c, there is a possible EoP due to a precondition check failure. 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-238785915References: N/A	6.7	More Details
CVE-2022-25627	An authenticated administrator who has physical access to the environment can carry out Remote Command Execution on Management Console in Symantec Identity Manager 14.4	6.7	More Details
CVE-2022-42523	In fillSetupDataCallInfo_V1_6 of ril_service_1_6.cpp, 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 kernelAndroid ID: A-243376893References: N/A	6.7	More Details
CVE-2022-20583	In ppmp_unprotect_mfcfw_buf of drm_fw.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege in S-EL1 with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-234859169References: N/A	6.7	More Details
CVE-2022-20581	In the Pixel camera driver, there is a possible use after free due to a logic error in the code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-245916120References: N/A	6.7	More Details
CVE-2022-20580	In ufdt_do_one_fixup of ufdt_overlay.c, 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 kernelAndroid ID: A-243629453References: N/A	6.7	More Details
CVE-2022-42501	In HexString2Value of util.cpp, 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 kernelAndroid ID: A-241231403References: N/A	6.7	More Details
CVE-2022-20579	In RadioImpl::setCdmaBroadcastConfig of ril_service_legacy.cpp, there is a possible stack clash leading to memory corruption. 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-243510139References: N/A	6.7	More Details
CVE-2022-20578	In RadioImpl::setGsmBroadcastConfig of ril_service_legacy.cpp, there is a possible stack clash leading to memory corruption. 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-243509749References: N/A	6.7	More Details
CVE-2022-20577	In OemSimAuthRequest::encode of wlandata.cpp, 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 kernelAndroid ID: A-241762281References: N/A	6.7	More Details
CVE-2022-20576	In externalOnRequest of rilapplication.cpp, 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 kernelAndroid ID: A-239701761References: N/A	6.7	More Details
CVE-2022-20572	In verity_target of dm-verity-target.c, there is a possible way to modify read-only files due to a missing permission check. 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-234475629References: Upstream kernel	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20571	In extract_metadata of dm-android-verity.c, there is a possible way to corrupt kernel memory 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-234030265References: Upstream kernel	6.7	More Details
CVE-2022-20514	In acquireFabricatedOverlayIterator, nextFabricatedOverlayInfos, and releaseFabricatedOverlayIterator of Idmap2Service.cpp, 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-13Android ID: A-245727875	6.7	More Details
CVE-2022-42519	In CdmaBroadcastSmsConfigsRequestData::encode of cdmasmsdata.cpp, there is a possible stack clash leading to memory corruption. 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-242540694References: N/A	6.7	More Details
CVE-2022-20549	In authToken2AidlVec of KeyMintUtils.cpp, 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-242702451	6.7	More Details
CVE-2022-20539	In parameterToHal of Effect.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the audio server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-237291425	6.7	More Details
CVE-2022-20505	In openFile of CallLogProvider.java, there is a possible permission bypass due to a path traversal error. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitationProduct: AndroidVersions: Android-13Android ID: A-225981754	6.7	More Details
CVE-2022-20509	In mapGrantorDescr of MessageQueueBase.h, 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-244713317	6.7	More Details
CVE-2022-42518	In BroadcastSmsConfigsRequestData::encode of smsdata.cpp, 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 kernelAndroid ID: A-242536278References: N/A	6.7	More Details
CVE-2022-42526	In ConvertUtf8ToUcs2 of radio_hal_utils.cpp, 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 kernelAndroid ID: A-243509880References: N/A	6.7	More Details
CVE-2022-42542	In phNxpNciHal_core_initialized of phNxpNciHal.cc, 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-231445184	6.7	More Details
CVE-2022-20504	In multiple locations of DreamManagerService.java, there is a missing permission check. This could lead to local escalation of privilege and dismissal of system dialogs with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-225878553	6.7	More Details
CVE-2022-42525	In fillSetupDataCallInfo_V1_6 of ril_service_1_6.cpp, 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 kernelAndroid ID: A-243509750References: N/A	6.7	More Details
CVE-2022-20546	In getCurrentConfigImpl of Effect.cpp, 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-240266798	6.7	More Details
CVE-2022-27498	A directory traversal vulnerability exists in the TicketTemplateActions.aspx GetTemplateAttachment functionality of Lansweeper lansweeper 10.1.1.0. A specially-crafted HTTP request can lead to arbitrary file read. An attacker can send an HTTP request to trigger this vulnerability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20553	In onCreate of LogAccessDialogActivity.java, there is a possible way to bypass a permission check due to a tapjacking/overlay attack. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-244155265	6.5	More Details
CVE-2022-4555	The WP Shamsi plugin for WordPress is vulnerable to authorization bypass due to a missing capability check on the deactivate() function hooked via init() in versions up to, and including, 4.1.0. This makes it possible for unauthenticated attackers to deactivate arbitrary plugins on the site. This can be used to deactivate security plugins that aids in exploiting other vulnerabilities.	6.5	More Details
CVE-2022-47407	An issue was discovered in the fp_masterquiz (aka Master-Quiz) extension before 2.2.1, and 3.x before 3.5.1, for TYPO3. An attacker can continue the quiz of a different user. In doing so, the attacker can view that user's answers and modify those answers.	6.5	More Details
CVE-2020-9420	The login password of the web administrative dashboard in Arcadyan Wifi routers VRV9506JAC23 is sent in cleartext, allowing an attacker to sniff and intercept traffic to learn the administrative credentials to the router.	6.5	More Details
CVE-2022-42852	The issue was addressed with improved memory handling. This issue is fixed in Safari 16.2, tvOS 16.2, macOS Ventura 13.1, iOS 15.7.2 and iPadOS 15.7.2, iOS 16.2 and iPadOS 16.2, watchOS 9.2. Processing maliciously crafted web content may result in the disclosure of process memory.	6.5	More Details
CVE-2021-28655	The improper Input Validation vulnerability in ""Move folder to Trash" feature of Apache Zeppelin allows an attacker to delete the arbitrary files. This issue affects Apache Zeppelin Apache Zeppelin version 0.9.0 and prior versions.	6.5	More Details
CVE-2022-4107	The SMSA Shipping for WooCommerce WordPress plugin before 1.0.5 does not have authorisation and proper CSRF checks, as well as does not validate the file to be downloaded, allowing any authenticated users, such as subscriber to download arbitrary file from the server	6.5	More Details
CVE-2022-23488	BigBlueButton is an open source web conferencing system. Versions prior to 2.4-rc-6 are vulnerable to Insertion of Sensitive Information Into Sent Data. The moderators-only webcams lock setting is not enforced on the backend, which allows an attacker to subscribe to viewers' webcams, even when the lock setting is applied. (The required streamId was being sent to all users even with lock setting applied). This issue is fixed in version 2.4-rc-6. There are no workarounds.	6.5	More Details
CVE-2022-23537	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. Buffer overread is possible when parsing a specially crafted STUN message with unknown attribute. The vulnerability affects applications that uses STUN including PJNATH and PJSUA-LIB. The patch is available as a commit in the master branch (2.13.1).	6.5	More Details
CVE-2022-4024	The Registration Forms WordPress plugin before 3.8.1.3 does not have authorisation and CSRF when deleting users via an init action handler, allowing unauthenticated attackers to delete arbitrary users (along with their posts)	6.5	More Details
CVE-2022-3961	The Directorist WordPress plugin before 7.4.4 does not prevent users with low privileges (like subscribers) from accessing sensitive system information.	6.5	More Details
CVE-2022-38708	IBM Cognos Analytics 11.1.7 11.2.0, and 11.2.1 could be vulnerable to a Server-Side Request Forgery Attack (SSRF) attack by constructing URLs from user-controlled data. This could enable attackers to make arbitrary requests to the internal network or to the local file system. IBM X-Force ID: 234180.	6.5	More Details
CVE-2022-43883	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could be vulnerable to a Log Injection attack by constructing URLs from user-controlled data. This could enable attackers to make arbitrary requests to the internal network or to the local file system. IBM X-Force ID: 240266.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23536	Cortex provides multi-tenant, long term storage for Prometheus. A local file inclusion vulnerability exists in Cortex versions 1.13.0, 1.13.1 and 1.14.0, where a malicious actor could remotely read local files as a result of parsing maliciously crafted Alertmanager configurations when submitted to the Alertmanager Set Configuration API. Only users of the Alertmanager service where `-experimental.alertmanager.enable-api` or `enable_api: true` is configured are affected. Affected Cortex users are advised to upgrade to patched versions 1.13.2 or 1.14.1. However as a workaround, Cortex administrators may reject Alertmanager configurations containing the `api_key_file` setting in the `opsgenie_configs` section before sending to the Set Alertmanager Configuration API.	6.5	More Details
CVE-2022-46402	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PairCon_rmSend with incorrect values.	6.5	More Details
CVE-2022-29511	A directory traversal vulnerability exists in the KnowledgebasePageActions.aspx ImportArticles functionality of Lansweeper lansweeper 10.1.1.0. A specially-crafted HTTP request can lead to arbitrary file read. An attacker can send an HTTP request to trigger this vulnerability.	6.5	More Details
CVE-2022-47551	Apiman 1.5.7 through 2.2.3.Final has insufficient checks for read permissions within the Apiman Manager REST API. The root cause of the issue is the Apiman project's accidental acceptance of a large contribution that was not fully compatible with the security model of Apiman versions before 3.0.0.Final. Because of this, 3.0.0.Final is not affected by the vulnerability.	6.5	More Details
CVE-2022-46698	A logic issue was addressed with improved checks. This issue is fixed in Safari 16.2, tvOS 16.2, iCloud for Windows 14.1, macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2, watchOS 9.2. Processing maliciously crafted web content may disclose sensitive user information.	6.5	More Details
CVE-2022-46695	A spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation. This issue is fixed in tvOS 16.2, macOS Ventura 13.1, iOS 15.7.2 and iPadOS 15.7.2, iOS 16.2 and iPadOS 16.2, watchOS 9.2. Visiting a website that frames malicious content may lead to UI spoofing.	6.5	More Details
CVE-2022-4427	Improper Input Validation vulnerability in OTRS AG OTRS, OTRS AG ((OTRS)) Community Edition allows SQL Injection via TicketSearch Webservice This issue affects OTRS: from 7.0.1 before 7.0.40 Patch 1, from 8.0.1 before 8.0.28 Patch 1; ((OTRS)) Community Edition: from 6.0.1 through 6.0.34.	6.5	More Details
CVE-2022-46139	TP-Link TL-WR940N V4 3.16.9 and earlier allows authenticated attackers to cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process.	6.5	More Details
CVE-2022-42343	Adobe Campaign version 7.3.1 (and earlier) and 8.3.9 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. A low-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction.	6.5	More Details
CVE-2022-4410	The Permalink Manager Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and including 2.2.20.3 due to improper output escaping on post/page/media titles. This makes it possible for attackers to inject arbitrary web scripts on the permalink-manager page if another plugin or theme is installed on the site that allows lower privileged users with unfiltered_html the ability to modify post/page titles with malicious web scripts.	6.4	More Details
CVE-2022-20567	In pppol2tp_create of l2tp_ppp.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-186777253References: Upstream kernel	6.4	More Details
CVE-2022-47549	An unprotected memory-access operation in optee_os in TrustedFirmware Open Portable Trusted Execution Environment (OP-TEE) before 3.20 allows a physically proximate adversary to bypass signature verification and install malicious trusted applications via electromagnetic fault injections.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23543	Silverware Games is a social network where people can play games online. Users can attach URLs to YouTube videos, the site will generate related `<iframe>` when the post will be published. The handler has some sort of protection so non-YouTube links can't be posted, as well as HTML tags are being stripped. However, it was still possible to add custom HTML attributes (e.g. `onclick=alert("xss")`) to the `<iframe>'. This issue was fixed in the version `1.1.34` and does not require any extra actions from our members. There has been no evidence that this vulnerability was used by anyone at this time.	6.3	More Details
CVE-2022-4592	A vulnerability was found in luckyshot CRMx and classified as critical. This issue affects the function get/save/delete/comment/commentdelete of the file index.php. The manipulation leads to sql injection. The attack may be initiated remotely. The name of the patch is 8c62d274986137d6a1d06958a6f75c3553f45f8f. It is recommended to apply a patch to fix this issue. The identifier VDB-216185 was assigned to this vulnerability.	6.3	More Details
CVE-2022-40264	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ICONICS/Mitsubishi Electric GENESIS64 versions 10.96 to 10.97.2 allows an unauthenticated attacker to create, tamper with or destroy arbitrary files by getting a legitimate user import a project package file crafted by the attacker.	6.3	More Details
CVE-2022-4493	A vulnerability classified as critical was found in scifio. Affected by this vulnerability is the function downloadAndUnpackResource of the file src/test/java/io/scif/util/DefaultSampleFilesService.java of the component ZIP File Handler. The manipulation leads to path traversal. The attack can be launched remotely. The name of the patch is fcb0dbca0ec72b22fe0c9ddc8abc9cb188a0ff31. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-215803.	6.3	More Details
CVE-2022-4494	A vulnerability, which was classified as critical, has been found in bspkrs MCPMappingViewer. Affected by this issue is the function extractZip of the file src/main/java/bspkrs/mmv/RemoteZipHandler.java of the component ZIP File Handler. The manipulation leads to path traversal. The attack may be launched remotely. The name of the patch is 6e602746c96b4756c271d080dae7d22ad804a1bd. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-215804.	6.3	More Details
CVE-2022-4594	A vulnerability was found in drogatkin TJWS2. It has been declared as critical. Affected by this vulnerability is the function deployWar of the file 1.x/src/rogatkin/web/WarRoller.java. The manipulation leads to path traversal. The attack can be launched remotely. The name of the patch is 1bac15c496ec54efe21ad7fab4e17633778582fc. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216187.	6.3	More Details
CVE-2021-4261	A vulnerability classified as critical has been found in pacman-canvas up to 1.0.5. Affected is the function addHighscore of the file data/db-handler.php. The manipulation leads to sql injection. It is possible to launch the attack remotely. Upgrading to version 1.0.6 is able to address this issue. The name of the patch is 29522c90ca1cebfce6453a5af5a45281d99b0646. It is recommended to upgrade the affected component. VDB-216270 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2021-4260	A vulnerability was found in oils-js. It has been declared as critical. This vulnerability affects unknown code of the file core/Web.js. The manipulation leads to open redirect. The attack can be initiated remotely. The name of the patch is fad8fbae824a7d367dacb90d56cb02c5cb999d42. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216268.	6.3	More Details
CVE-2022-4583	A vulnerability was found in jLEMS. It has been declared as critical. Affected by this vulnerability is the function unpackJar of the file src/main/java/org/lemsml/jlems/io/util/JUtil.java. The manipulation leads to path traversal. The attack can be launched remotely. The name of the patch is 8c224637d7d561076364a9e3c2c375daeaf463dc. It is recommended to apply a patch to fix this issue. The identifier VDB-216169 was assigned to this vulnerability.	6.3	More Details
CVE-2021-4246	A vulnerability was found in roxlukas LMeve and classified as critical. Affected by this issue is some unknown functionality of the component Login Page. The manipulation of the argument X-Forwarded-For leads to sql injection. The attack may be launched remotely. The name of the patch is 29e1ead3bb1c1fad53b77dfc14534496421c5b5d. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216176.	6.3	More Details
CVE-2022-4584	A vulnerability was found in Axiomatic Bento4 up to 1.6.0-639. It has been rated as critical. Affected by this issue is some unknown functionality of the component mp42aac. The manipulation leads to heap-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-216170 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36618	A vulnerability classified as critical has been found in Furqan node-whois. Affected is an unknown function of the file index.coffee. The manipulation leads to improperly controlled modification of object prototype attributes ('prototype pollution'). It is possible to launch the attack remotely. The name of the patch is 46ccc2aee8d063c7b6b4dee2c2834113b7286076. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216252.	6.3	More Details
CVE-2022-43382	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a local user with elevated privileges to exploit a vulnerability in the lpd daemon to cause a denial of service. IBM X-Force ID: 238641.	6.2	More Details
CVE-2022-43875	IBM Financial Transaction Manager for SWIFT Services for Multiplatforms 3.2.4 could allow an authenticated user to lock additional RM authorizations, resulting in a denial of service on displaying or managing these authorizations. IBM X-Force ID: 240034.	6.2	More Details
CVE-2021-33640	After tar_close(), libtar.c releases the memory pointed to by pointer t. After tar_close() is called in the list() function, it continues to use pointer t: free_longlink_longname(t->th_buf) . As a result, the released memory is used (use-after-free).	6.2	More Details
CVE-2022-38662	In HCL Digital Experience, URLs can be constructed to redirect users to untrusted sites.	6.1	More Details
CVE-2022-46287	Cross-site scripting vulnerability in DENSHI NYUSATSU CORE SYSTEM v6 R4 and earlier allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details
CVE-2022-41993	Cross-site scripting vulnerability in DENSHI NYUSATSU CORE SYSTEM v6 R4 and earlier allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details
CVE-2022-44235	Beijing Zed-3 Technologies Co.,Ltd VoIP simplicIty ASG 8.5.0.17807 (20181130-16:12) is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2020-20589	Cross Site Scripting (XSS) vulnerability in FeehiCMS 2.0.8 allows remote attackers to run arbitrary code via tha lang attribute of an html tag.	6.1	More Details
CVE-2022-23515	Loofah is a general library for manipulating and transforming HTML/XML documents and fragments, built on top of Nokogiri. Loofah >= 2.1.0, < 2.19.1 is vulnerable to cross-site scripting via the image/svg+xml media type in data URIs. This issue is patched in version 2.19.1.	6.1	More Details
CVE-2022-32763	A cross-site scripting (xss) sanitization vulnerability bypass exists in the SanitizeHtml functionality of Lansweeper lansweeper 10.1.1.0. A specially-crafted HTTP request can lead to arbitrary Javascript code injection. An attacker can send an HTTP request to trigger this vulnerability.	6.1	More Details
CVE-2020-21219	Cross Site Scripting (XSS) vulnerability in Netgate pf Sense 2.4.4-Release-p3 and Netgate ACME package 0.6.3 allows remote attackers to to run arbitrary code via the RootFolder field to acme_certificate_edit.php page of the ACME package.	6.1	More Details
CVE-2020-36607	Cross Site Scripting (XSS) vulnerability in FeehiCMS 2.0.8 allows remote attackers to run arbitrary code via tha lang attribute of an html tag.	6.1	More Details
CVE-2021-36572	Cross Site Scripting (XSS) vulnerability in Feehi CMS thru 2.1.1 allows attackers to run arbitrary code via the user name field of the login page.	6.1	More Details
CVE-2022-46288	Open redirect vulnerability in DENSHI NYUSATSU CORE SYSTEM v6 R4 and earlier allows a remote unauthenticated attacker to redirect a user to an arbitrary web site and conduct a phishing attack by having a user to access a specially crafted URL.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23474	Editor.js is a block-style editor with clean JSON output. Versions prior to 2.26.0 are vulnerable to Code Injection via pasted input. The processHTML method passes pasted input into wrapper's innerHTML. This issue is patched in version 2.26.0.	6.1	More Details
CVE-2022-4503	Cross-site Scripting (XSS) - Generic in GitHub repository openemr/openemr prior to 7.0.0.2.	6.1	More Details
CVE-2022-4502	Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.2.	6.1	More Details
CVE-2022-47500	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Apache Software Foundation Apache Helix UI component.This issue affects Apache Helix all releases from 0.8.0 to 1.0.4. Solution: removed the the forward component since it was improper designed for UI embedding. User please upgrade to 1.1.0 to fix this issue.	6.1	More Details
CVE-2022-40743	Improper Input Validation vulnerability for the xdebug plugin in Apache Software Foundation Apache Traffic Server can lead to cross site scripting and cache poisoning attacks.This issue affects Apache Traffic Server: 9.0.0 to 9.1.3. Users should upgrade to 9.1.4 or later versions.	6.1	More Details
CVE-2022-46073	Helmet Store Showroom 1.0 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details
CVE-2022-3073	Quanos "SCHEMA ST4" example web templates in version Bootstrap 2019 v2/2021 v1/2022 v1/2022 SP1 v1 or below are prone to JavaScript injection allowing a remote attacker to hijack existing sessions to e.g. other web services in the same environment or execute scripts in the users browser environment. The affected script is '*-schema.js'.	6.1	More Details
CVE-2022-23518	rails-html-sanitizer is responsible for sanitizing HTML fragments in Rails applications. Versions >= 1.0.3, < 1.4.4 are vulnerable to cross-site scripting via data URIs when used in combination with Loofah >= 2.1.0. This issue is patched in version 1.4.4.	6.1	More Details
CVE-2022-39160	IBM Cognos Analytics 11.2.1, 11.2.0, and 11.1.7 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 235064.	6.1	More Details
CVE-2022-4615	Cross-site Scripting (XSS) - Reflected in GitHub repository openemr/openemr prior to 7.0.0.2.	6.1	More Details
CVE-2022-23520	rails-html-sanitizer is responsible for sanitizing HTML fragments in Rails applications. Prior to version 1.4.4, there is a possible XSS vulnerability with certain configurations of Rails::Html::Sanitizer due to an incomplete fix of CVE-2022-32209. Rails::Html::Sanitizer may allow an attacker to inject content if the application developer has overridden the sanitizer's allowed tags to allow both "select" and "style" elements. Code is only impacted if allowed tags are being overridden. This issue is patched in version 1.4.4. All users overriding the allowed tags to include both "select" and "style" should either upgrade or use this workaround: Remove either "select" or "style" from the overridden allowed tags. NOTE: Code is _not_ impacted if allowed tags are overridden using either the :tags option to the Action View helper method sanitize or the :tags option to the instance method SafeListSanitizer#sanitize.	6.1	More Details
CVE-2022-36223	In Emby Server 4.6.7.0, the playlist name field is vulnerable to XSS stored where it is possible to steal the administrator access token and flip or steal the media server administrator account.	6.1	More Details
CVE-2022-38659	In specific scenarios, on Windows the operator credentials may be encrypted in a manner that is not completely machine-dependent.	6.0	More Details
CVE-2022-26579	PAX A930 device with PayDroid_7.1.1_Virgo_V04.3.26T1_20210419 can allow a root privileged attacker to install unsigned packages. The attacker must have shell access to the device and gain root privileges in order to exploit this vulnerability.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23500	TYPO3 is an open source PHP based web content management system. In versions prior to 9.5.38, 10.4.33, 11.5.20, and 12.1.1, requesting invalid or non-existing resources via HTTP triggers the page error handler, which again could retrieve content to be shown as an error message from another page. This leads to a scenario in which the application is calling itself recursively - amplifying the impact of the initial attack until the limits of the web server are exceeded. This vulnerability is very similar, but not identical, to the one described in CVE-2021-21359. This issue is patched in versions 9.5.38 ELTS, 10.4.33, 11.5.20 or 12.1.1.	5.9	More Details
CVE-2022-23501	TYPO3 is an open source PHP based web content management system. In versions prior to 8.7.49, 9.5.38, 10.4.33, 11.5.20, and 12.1.1 TYPO3 is vulnerable to Improper Authentication. Restricting frontend login to specific users, organized in different storage folders (partitions), can be bypassed. A potential attacker might use this ambiguity in usernames to get access to a different account - however, credentials must be known to the adversary. This issue is patched in versions 8.7.49 ELTS, 9.5.38 ELTS, 10.4.33, 11.5.20, 12.1.1.	5.9	More Details
CVE-2022-3590	WordPress is affected by an unauthenticated blind SSRF in the pingback feature. Because of a TOCTOU race condition between the validation checks and the HTTP request, attackers can reach internal hosts that are explicitly forbidden.	5.9	More Details
CVE-2022-46768	Arbitrary file read vulnerability exists in Zabbix Web Service Report Generation, which listens on the port 10053. The service does not have proper validation for URL parameters before reading the files.	5.9	More Details
CVE-2022-32531	The Apache Bookkeeper Java Client (before 4.14.6 and also 4.15.0) does not close the connection to the bookkeeper server when TLS hostname verification fails. This leaves the bookkeeper client vulnerable to a man in the middle attack. The problem affects BookKeeper client prior to versions 4.14.6 and 4.15.1.	5.9	More Details
CVE-2022-23530	GuardDog is a CLI tool to identify malicious PyPI packages. Versions prior to v0.1.8 are vulnerable to arbitrary file write when scanning a specially-crafted remote PyPI package. Extracting files using shutil.unpack_archive() from a potentially malicious tarball without validating that the destination file path is within the intended destination directory can cause files outside the destination directory to be overwritten. This issue is patched in version 0.1.8. Potential workarounds include using a safer module, like zipfile, and validating the location of the extracted files and discarding those with malicious paths.	5.8	More Details
CVE-2022-23531	GuardDog is a CLI tool to identify malicious PyPI packages. Versions prior to 0.1.5 are vulnerable to Relative Path Traversal when scanning a specially-crafted local PyPI package. Running GuardDog against a specially-crafted package can allow an attacker to write an arbitrary file on the machine where GuardDog is executed due to a path traversal vulnerability when extracting the .tar.gz file of the package being scanned, which exists by design in the tarfile.TarFile.extractall function. This issue is patched in version 0.1.5.	5.8	More Details
CVE-2022-44643	A vulnerability in the label-based access control of Grafana Labs Grafana Enterprise Metrics allows an attacker more access than intended. If an access policy which has label selector restrictions also has been granted access to all tenants in the system, the label selector restrictions will not be applied when using this policy with the affected versions of the software. This issue affects: Grafana Labs Grafana Enterprise Metrics GEM 1.X versions prior to 1.7.1 on AMD64; GEM 2.X versions prior to 2.3.1 on AMD64.	5.7	More Details
CVE-2022-41964	BigBlueButton is an open source web conferencing system. This vulnerability only affects release candidates of BigBlueButton 2.4. The attacker can start a subscription for poll results before starting an anonymous poll, and use this subscription to see individual responses in the anonymous poll. The attacker had to be a meeting presenter. This issue is patched in version 2.4.0. There are no workarounds.	5.7	More Details
CVE-2022-23504	TYPO3 is an open source PHP based web content management system. Versions prior to 9.5.38, 10.4.33, 11.5.20, and 12.1.1 are subject to Sensitive Information Disclosure. Due to the lack of handling user-submitted YAML placeholder expressions in the site configuration backend module, attackers could expose sensitive internal information, such as system configuration or HTTP request messages of other website visitors. A valid backend user account having administrator privileges is needed to exploit this vulnerability. This issue has been patched in versions 9.5.38 ELTS, 10.4.33, 11.5.20, 12.1.1.	5.7	More Details
CVE-2021-4248	A vulnerability was found in kapetan dns up to 6.1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file DNS/Protocol/Request.cs. The manipulation leads to insufficient entropy in prng. The attack may be launched remotely. Upgrading to version 7.0.0 is able to address this issue. The name of the patch is cf7105aa2aae90d6656088fe5a8ee1d5730773b6. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216188.	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36619	A vulnerability was found in multimon-ng. It has been rated as critical. This issue affects the function add_ch of the file demod_flex.c. The manipulation of the argument ch leads to format string. Upgrading to version 1.2.0 is able to address this issue. The name of the patch is e5a51c508ef952e81a6da25b43034dd1ed023c07. It is recommended to upgrade the affected component. The identifier VDB-216269 was assigned to this vulnerability.	5.5	More Details
CVE-2022-44498	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (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-2022-44499	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (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-2022-44500	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (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-2022-44502	Adobe Illustrator versions 26.5.1 (and earlier), and 27.0 (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-2022-4326	Improper preservation of permissions vulnerability in Trellix Endpoint Agent (xAgent) prior to V35.31.22 on Windows allows a local user with administrator privileges to bypass the product protection to uninstall the agent via incorrectly applied permissions in the removal protection functionality.	5.5	More Details
CVE-2022-4566	A vulnerability, which was classified as critical, has been found in y_project RuoYi 4.7.5. This issue affects some unknown processing of the file com/ruoyi/generator/controller/GenController. The manipulation leads to sql injection. The name of the patch is 167970e5c4da7bb46217f576dc50622b83f32b40. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-215975.	5.5	More Details
CVE-2022-4589	A vulnerability has been found in cyface Terms and Conditions Module up to 2.0.9 and classified as problematic. Affected by this vulnerability is the function returnTo of the file termsandconditions/views.py. The manipulation leads to open redirect. The attack can be launched remotely. Upgrading to version 2.0.10 is able to address this issue. The name of the patch is 03396a1c2e0af95e12a45c5faef7e47a4b513e1a. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216175.	5.5	More Details
CVE-2022-4607	A vulnerability was found in 3D City Database OGC Web Feature Service up to 5.2.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to xml external entity reference. Upgrading to version 5.2.1 is able to address this issue. The name of the patch is 246f4e2a97ad81491c00a7ed72ce5e7c7f75050a. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216215.	5.5	More Details
CVE-2021-4262	A vulnerability classified as critical was found in laravel-jqgrid. Affected by this vulnerability is the function getRows of the file src/Mgallegos/LaravelJqgrid/Repositories/EloquentRepositoryAbstract.php. The manipulation leads to sql injection. The name of the patch is fbc2d94f43d0dc772767a5bdb2681133036f935e. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216271.	5.5	More Details
CVE-2022-47512	Sensitive information was stored in plain text in a file that is accessible by a user with a local account in Hybrid Cloud Observability (HCO)/ SolarWinds Platform 2022.4. No other versions are affected	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4619	The Sidebar Widgets by CodeLights plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Extra CSS class' parameter in versions up to, and including, 1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2022-41590	Some smartphones have authentication-related (including session management) vulnerabilities as the setup wizard is bypassed. Successful exploitation of this vulnerability affects the smartphone availability.	5.5	More Details
CVE-2022-42535	In a query in MmsSmsProvider.java, there is a possible access to restricted tables due to SQL injection. 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-224770183	5.5	More Details
CVE-2022-20609	In Pixel cellular firmware, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239240808References: N/A	5.5	More Details
CVE-2022-3114	An issue was discovered in the Linux kernel through 5.16-rc6. imx_register_uart_clocks in drivers/clk/imx/clk.c lacks check of the return value of kcalloc() and will cause the null pointer dereference.	5.5	More Details
CVE-2022-20608	In Pixel cellular firmware, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239239246References: N/A	5.5	More Details
CVE-2022-20592	In ppmp_validate_secbuf of drm_fw.c, there is a possible information disclosure 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 kernelAndroid ID: A-238976908References: N/A	5.5	More Details
CVE-2022-20591	In ppmpu_set of ppmpu.c, there is a possible information disclosure due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238939706References: N/A	5.5	More Details
CVE-2022-20590	In valid_va_sec_mfc_check of drm_access_control.c, there is a possible information disclosure 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 kernelAndroid ID: A-238932493References: N/A	5.5	More Details
CVE-2022-3110	An issue was discovered in the Linux kernel through 5.16-rc6. _rtw_init_xmit_priv in drivers/staging/r8188eu/core/rtw_xmit.c lacks check of the return value of rtw_alloc_hwxmits() and will cause the null pointer dereference.	5.5	More Details
CVE-2022-20575	In read_ppmpu_info of drm_fw.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-237585040References: N/A	5.5	More Details
CVE-2022-20574	In sec_sysmmu_info of drm_fw.c, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-237582191References: N/A	5.5	More Details
CVE-2022-20570	Product: AndroidVersions: Android kernelAndroid ID: A-230660904References: N/A	5.5	More Details
CVE-2022-3104	An issue was discovered in the Linux kernel through 5.16-rc6. lkdtm_ARRAY_BOUNDS in drivers/misc/lkdtm/bugs.c lacks check of the return value of kmalloc() and will cause the null pointer dereference.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3105	An issue was discovered in the Linux kernel through 5.16-rc6. uapi_finalize in drivers/infiniband/core/uverbs_uapi.c lacks check of kmalloc_array().	5.5	More Details
CVE-2022-20552	In btif_a2dp_sink_command_ready of btif_a2dp_sink.cc, there is a possible out of bounds read due to a use after free. 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-243922806	5.5	More Details
CVE-2022-3106	An issue was discovered in the Linux kernel through 5.16-rc6. ef100_update_stats in drivers/net/ethernet/sfc/ef100_nic.c lacks check of the return value of kmalloc().	5.5	More Details
CVE-2022-3107	An issue was discovered in the Linux kernel through 5.16-rc6. netvsc_get_ethtool_stats in drivers/net/hyperv/netvsc_drv.c lacks check of the return value of kvmalloc_array() and will cause the null pointer dereference.	5.5	More Details
CVE-2022-20199	In multiple locations of NfcService.java, there is a possible disclosure of NFC tags due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-199291025	5.5	More Details
CVE-2022-3108	An issue was discovered in the Linux kernel through 5.16-rc6. kfd_parse_subtype_iolink in drivers/gpu/drm/amd/amdkfd/kfd_crat.c lacks check of the return value of kmemdup().	5.5	More Details
CVE-2022-3115	An issue was discovered in the Linux kernel through 5.16-rc6. malidp_crtc_reset in drivers/gpu/drm/arm/malidp_crtc.c lacks check of the return value of kzalloc() and will cause the null pointer dereference.	5.5	More Details
CVE-2022-20510	In getNearbyNotificationStreamingPolicy of DevicePolicyManagerService.java, there is a possible way to learn about the notification streaming policy of other users 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-235822336	5.5	More Details
CVE-2022-20511	In getNearbyAppStreamingPolicy of DevicePolicyManagerService.java, there is 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-235821829	5.5	More Details
CVE-2022-20513	In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-244569759	5.5	More Details
CVE-2022-20515	In onPreferenceClick of AccountTypePreferenceLoader.java, there is a possible way to retrieve protected files from the Settings app due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-220733496	5.5	More Details
CVE-2022-20517	In getMessagesByPhoneNumber of MmsSmsProvider.java, there is a possible access to restricted tables due to SQL injection. 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-224769956	5.5	More Details
CVE-2022-20518	In query of MmsSmsProvider.java, there is a possible access to restricted tables due to SQL injection. 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-224770203	5.5	More Details
CVE-2022-3113	An issue was discovered in the Linux kernel through 5.16-rc6. mtk_vcodec_fw_vpu_init in drivers/media/platform/mtk-vcodec/mtk_vcodec_fw_vpu.c lacks check of the return value of devm_kzalloc() and will cause the null pointer dereference.	5.5	More Details
CVE-2022-3112	An issue was discovered in the Linux kernel through 5.16-rc6. amvdec_set_canvases in drivers/staging/media/meson/vdec/vdec_helpers.c lacks check of the return value of kzalloc() and will cause the null pointer dereference.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20523	In IncFs_GetFilledRangesStartingFrom of incfs.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-228222508	5.5	More Details
CVE-2022-3111	An issue was discovered in the Linux kernel through 5.16-rc6. free_charger_irq() in drivers/power/supply/wm8350_power.c lacks free of WM8350_IRQ_CHG_FAST_RDY, which is registered in wm8350_init_charger().	5.5	More Details
CVE-2022-20527	In HalCoreCallback of halcore.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure from the NFC firmware with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-229994861	5.5	More Details
CVE-2022-20531	In Telecom, 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.	5.5	More Details
CVE-2022-20604	In SAECOMM_SetDcnIdForPlmn of SAECOMM_DbManagement.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure from a single device with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-230463606References: N/A	5.5	More Details
CVE-2022-20538	In getSmsRoleHolder of RoleService.java, 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-235601770	5.5	More Details
CVE-2022-42821	A logic issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.6.2, macOS Big Sur 11.7.2, macOS Ventura 13. An app may bypass Gatekeeper checks.	5.5	More Details
CVE-2022-32916	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 16. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2022-4519	The WP User plugin for WordPress is vulnerable to Stored Cross-Site Scripting via its settings parameters in versions up to, and including, 7.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2022-42853	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Ventura 13.1. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2022-42854	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6.2, macOS Ventura 13.1. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2022-42846	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.2 and iPadOS 16.2, iOS 15.7.2 and iPadOS 15.7.2. Parsing a maliciously crafted video file may lead to unexpected system termination.	5.5	More Details
CVE-2021-4245	A vulnerability classified as problematic has been found in chbrown rfc6902. This affects an unknown part of the file pointer.ts. The manipulation leads to improperly controlled modification of object prototype attributes ('prototype pollution'). The exploit has been disclosed to the public and may be used. The name of the patch is c006ce9faa43d31edb34924f1df7b79c137096cf. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-215883.	5.5	More Details
CVE-2022-46702	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.2 and iPadOS 16.2. An app may be able to disclose kernel memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46692	A logic issue was addressed with improved state management. This issue is fixed in Safari 16.2, tvOS 16.2, iCloud for Windows 14.1, iOS 15.7.2 and iPadOS 15.7.2, macOS Ventura 13.1, iOS 16.2 and iPadOS 16.2, watchOS 9.2. Processing maliciously crafted web content may bypass Same Origin Policy.	5.5	More Details
CVE-2022-42865	This issue was addressed by enabling hardened runtime. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1, tvOS 16.2, watchOS 9.2. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2022-42866	The issue was addressed with improved handling of caches. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1, tvOS 16.2, watchOS 9.2. An app may be able to read sensitive location information.	5.5	More Details
CVE-2022-42851	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.2 and iPadOS 16.2, tvOS 16.2. Parsing a maliciously crafted TIFF file may lead to disclosure of user information.	5.5	More Details
CVE-2022-42859	Multiple issues were addressed by removing the vulnerable code. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1, watchOS 9.2. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2022-42843	This issue was addressed with improved data protection. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1, tvOS 16.2, watchOS 9.2. A user may be able to view sensitive user information.	5.5	More Details
CVE-2022-42862	This issue was addressed by removing the vulnerable code. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2022-46400	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) allows attackers to bypass passkey entry in legacy pairing.	5.4	More Details
CVE-2021-39427	Cross site scripting vulnerability in 188Jianzhan 2.10 allows attackers to execute arbitrary code via the username parameter to /admin/reg.php.	5.4	More Details
CVE-2021-39428	Cross Site Scripting (XSS) vulnerability in Users.php in eyoucms 1.5.4 allows remote attackers to run arbitrary code and gain escalated privilege via the filename for edit_users_head_pic.	5.4	More Details
CVE-2022-31683	Concourse (7.x.y prior to 7.8.3 and 6.x.y prior to 6.7.9) contains an authorization bypass issue. A Concourse user can send a request with body including :team_name=team2 to bypass team scope check to gain access to certain resources belong to any other team.	5.4	More Details
CVE-2022-23507	Tendermint is a high-performance blockchain consensus engine for Byzantine fault tolerant applications. Versions prior to 0.28.0 contain a potential attack via Improper Verification of Cryptographic Signature, affecting anyone using the tendermint-light-client and related packages to perform light client verification (e.g. IBC-rs, Hermes). The light client does not check that the chain IDs of the trusted and untrusted headers match, resulting in a possible attack vector where someone who finds a header from an untrusted chain that satisfies all other verification conditions (e.g. enough overlapping validator signatures) could fool a light client. The attack vector is currently theoretical, and no proof-of-concept exists yet to exploit it on live networks. This issue is patched in version 0.28.0. There are no workarounds.	5.4	More Details
CVE-2022-47406	An issue was discovered in the fe_change_pwd (aka Change password for frontend users) extension before 2.0.5, and 3.x before 3.0.3, for TYPO3. The extension fails to revoke existing sessions for the current user when the password has been changed.	5.4	More Details
CVE-2022-4058	The Photo Gallery by 10Web WordPress plugin before 1.8.3 does not validate and escape some parameters before outputting them back in in JS code later on in another page, which could lead to Stored XSS issue when an attacker makes a logged in admin open a malicious URL or page under their control.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3985	The Videojs HTML5 Player WordPress plugin before 1.1.9 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-3987	The Responsive Lightbox2 WordPress plugin before 1.0.4 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-3986	The WP Stripe Checkout WordPress plugin before 1.2.2.21 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-3984	The Flowplayer Video Player WordPress plugin before 1.0.5 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-3983	The Checkout for PayPal WordPress plugin before 1.0.14 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2022-40373	Cross Site Scripting (XSS) vulnerability in FeehiCMS 2.1.1 allows remote attackers to run arbitrary code via upload of crafted XML file.	5.4	More Details
CVE-2022-3937	The Easy Video Player WordPress plugin before 1.2.2.3 does not sanitize and escapes some parameters, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks.	5.4	More Details
CVE-2022-40002	Cross Site Scripting (XSS) vulnerability in FeehiCMS-2.1.1 allows remote attackers to run arbirtary code via the callback parameter to /cms/notify.	5.4	More Details
CVE-2022-40001	Cross Site Scripting (XSS) vulnerability in FeehiCMS-2.1.1 allows remote attackers to run arbitrary code via the title field of the create article page.	5.4	More Details
CVE-2022-40000	Cross Site Scripting (XSS) vulnerability in FeehiCMS-2.1.1 allows remote attackers to run arbitrary code via the username field of the admin log in page.	5.4	More Details
CVE-2022-4609	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.0.	5.4	More Details
CVE-2022-23502	TYPO3 is an open source PHP based web content management system. In versions prior to 10.4.33, 11.5.20, and 12.1.1, When users reset their password using the corresponding password recovery functionality, existing sessions for that particular user account were not revoked. This applied to both frontend user sessions and backend user sessions. This issue is patched in versions 10.4.33, 11.5.20, 12.1.1.	5.4	More Details
CVE-2020-9419	Multiple stored cross-site scripting (XSS) vulnerabilities in Arcadyan Wifi routers VRV9506JAC23 allow remote attackers to inject arbitrary web script or HTML via the hostName and domain_name parameters present in the LAN configuration section of the administrative dashboard.	5.4	More Details
CVE-2022-42141	Delta Electronics DX-2100-L1-CN 2.42 is vulnerable to Cross Site Scripting (XSS) via lform/urlfilter.	5.4	More Details
CVE-2021-36573	File Upload vulnerability in Feehi CMS thru 2.1.1 allows attackers to run arbitrary code via crafted image upload.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35693	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-46870	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache Zeppelin allows logged-in users to execute arbitrary javascript in other users' browsers. This issue affects Apache Zeppelin before 0.8.2. Users are recommended to upgrade to a supported version of Zeppelin.	5.4	More Details
CVE-2022-30679	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-4614	Cross-site Scripting (XSS) - Stored in GitHub repository alagrede/znote-app prior to 1.7.11.	5.4	More Details
CVE-2022-44474	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-44471	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-44470	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-44467	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-44466	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-44465	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-44463	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42365	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42364	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-28703	A stored cross-site scripting vulnerability exists in the HdConfigActions.aspx altertextlanguages functionality of Lansweeper lansweeper 10.1.1.0. A specially-crafted HTTP request can lead to arbitrary Javascript code injection. An attacker can send an HTTP request to trigger this vulnerability.	5.4	More Details
CVE-2022-42357	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-45033	A cross-site scripting (XSS) vulnerability in Expense Tracker 1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Chat text field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42356	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42354	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42352	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42350	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42349	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42348	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42346	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42345	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-35695	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-46401	The Microchip RN4870 module firmware 1.43 (and the Microchip PIC LightBlue Explorer Demo 4.2 DT100112) accepts PauseEncReqPlainText before pairing is complete.	5.4	More Details
CVE-2022-42362	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-44473	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42366	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42367	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-42360	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-44462	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38106	This vulnerability happens in the web client versions 15.3.0 to Serv-U 15.3.1. This vulnerability affects the directory creation function.	5.4	More Details
CVE-2022-35696	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-35694	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-4572	A vulnerability, which was classified as problematic, has been found in UBI Reader up to 0.8.0. Affected by this issue is the function ubireader_extract_files of the file ubireader/ubifs/output.py of the component UBIFS File Handler. The manipulation leads to path traversal. The attack may be launched remotely. Upgrading to version 0.8.5 is able to address this issue. The name of the patch is d5d68e6b1b9f7070c29df5f67fc060f579ae9139. It is recommended to upgrade the affected component. VDB-216146 is the identifier assigned to this vulnerability.	5.4	More Details
CVE-2022-44468	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-44469	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged 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.	5.4	More Details
CVE-2022-4605	Cross-site Scripting (XSS) - Stored in GitHub repository flatpressblog/flatpress prior to 1.3.	5.4	More Details
CVE-2022-46392	An issue was discovered in Mbed TLS before 2.28.2 and 3.x before 3.3.0. An adversary with access to precise enough information about memory accesses (typically, an untrusted operating system attacking a secure enclave) can recover an RSA private key after observing the victim performing a single private-key operation, if the window size (MBEDTLS_MPI_WINDOW_SIZE) used for the exponentiation is 3 or smaller.	5.3	More Details
CVE-2022-25626	An unauthenticated user can access Identity Manager’s management console specific page URLs. However, the system doesn’t allow the user to carry out server side tasks without a valid web session.	5.3	More Details
CVE-2022-43887	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could be vulnerable to sensitive information exposure by passing API keys to log files. If these keys contain sensitive information, it could lead to further attacks. IBM X-Force ID: 240450.	5.3	More Details
CVE-2022-32833	An issue existed with the file paths used to store website data. The issue was resolved by improving how website data is stored. This issue is fixed in iOS 16. An unauthorized user may be able to access browsing history.	5.3	More Details
CVE-2022-4511	A vulnerability has been found in RainyGao DocSys and classified as critical. Affected by this vulnerability is an unknown functionality of the component com.DocSystem.controller.UserController#getUserImg. The manipulation leads to path traversal: '../filedir'. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-215851.	5.3	More Details
CVE-2020-24855	Directory Traversal vulnerability in easywebpack-cli before 4.5.2 allows attackers to obtain sensitive information via crafted GET request.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23524	Helm is a tool for managing Charts, pre-configured Kubernetes resources. Versions prior to 3.10.3 are subject to Uncontrolled Resource Consumption, resulting in Denial of Service. Input to functions in the _strvals_ package can cause a stack overflow. In Go, a stack overflow cannot be recovered from. Applications that use functions from the _strvals_ package in the Helm SDK can have a Denial of Service attack when they use this package and it panics. This issue has been patched in 3.10.3. SDK users can validate strings supplied by users won't create large arrays causing significant memory usage before passing them to the _strvals_ functions.	5.3	More Details
CVE-2022-43872	IBM Financial Transaction Manager 3.2.4 authorization checks are done incorrectly for some HTTP requests which allows getting unauthorized technical information (e.g. event log entries) about the FTM SWIFT system. IBM X-Force ID: 239708.	5.3	More Details
CVE-2022-37392	Improper Check for Unusual or Exceptional Conditions vulnerability in handling the requests to Apache Traffic Server. This issue affects Apache Traffic Server 8.0.0 to 9.1.2.	5.3	More Details
CVE-2022-23525	Helm is a tool for managing Charts, pre-configured Kubernetes resources. Versions prior to 3.10.3 are subject to NULL Pointer Dereference in the _repo_package. The _repo_ package contains a handler that processes the index file of a repository. For example, the Helm client adds references to chart repositories where charts are managed. The _repo_ package parses the index file of the repository and loads it into structures Go can work with. Some index files can cause array data structures to be created causing a memory violation. Applications that use the _repo_ package in the Helm SDK to parse an index file can suffer a Denial of Service when that input causes a panic that cannot be recovered from. The Helm Client will panic with an index file that causes a memory violation panic. Helm is not a long running service so the panic will not affect future uses of the Helm client. This issue has been patched in 3.10.3. SDK users can validate index files that are correctly formatted before passing them to the _repo_ functions.	5.3	More Details
CVE-2022-23526	Helm is a tool for managing Charts, pre-configured Kubernetes resources. Versions prior to 3.10.3 are subject to NULL Pointer Dereference in the_chartutil_ package that can cause a segmentation violation. The _chartutil_ package contains a parser that loads a JSON Schema validation file. For example, the Helm client when rendering a chart will validate its values with the schema file. The _chartutil_ package parses the schema file and loads it into structures Go can work with. Some schema files can cause array data structures to be created causing a memory violation. Applications that use the _chartutil_ package in the Helm SDK to parse a schema file can suffer a Denial of Service when that input causes a panic that cannot be recovered from. Helm is not a long running service so the panic will not affect future uses of the Helm client. This issue has been patched in 3.10.3. SDK users can validate schema files that are correctly formatted before passing them to the _chartutil_ functions.	5.3	More Details
CVE-2022-32943	The issue was addressed with improved bounds checks. This issue is fixed in iOS 16.2 and iPadOS 16.2, macOS Ventura 13.1. Shake-to-undo may allow a deleted photo to be re-surfaced without authentication.	5.3	More Details
CVE-2022-47547	GossipSub 1.1, as used for Ethereum 2.0, allows a peer to maintain a positive score (and thus not be pruned from the network) even though it continuously misbehaves by never forwarding topic messages.	5.3	More Details
CVE-2022-31701	VMware Workspace ONE Access and Identity Manager contain a broken authentication vulnerability. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 5.3.	5.3	More Details
CVE-2022-46318	The HAware module has a function logic error. Successful exploitation of this vulnerability will affect the account removal function in Settings.	5.3	More Details
CVE-2022-20530	In strings.xml, there is a possible permission bypass due to a misleading string. This could lead to remote information disclosure of call logs with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-231585645	5.3	More Details
CVE-2022-46313	The sensor privacy module has an authentication vulnerability. Successful exploitation of this vulnerability may cause unavailability of the smartphone's camera and microphone.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38391	IBM Spectrum Control 5.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 233982.	5.1	More Details
CVE-2022-20521	In sdpu_find_most_specific_service_uuid of sdp_utils.cc, there is a possible way to crash Bluetooth due to a missing null check. This could lead to local denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-227203684	5.0	More Details
CVE-2022-39304	ghinstallation provides transport, which implements http.RoundTripper to provide authentication as an installation for GitHub Apps. In ghinstallation version 1, when the request to refresh an installation token failed, the HTTP request and response would be returned for debugging. The request contained the bearer JWT for the App, and was returned back to clients. This token is short lived (10 minute maximum). This issue has been patched and is available in version 2.0.0.	5.0	More Details
CVE-2021-4259	A vulnerability was found in phpRedisAdmin up to 1.16.1. It has been classified as problematic. This affects the function authHttpDigest of the file includes/login.inc.php. The manipulation of the argument response leads to use of wrong operator in string comparison. Upgrading to version 1.16.2 is able to address this issue. The name of the patch is 31aa7661e6db6f4dffbf9a635817832a0a11c7d9. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216267.	5.0	More Details
CVE-2022-4613	A vulnerability was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome and classified as critical. This issue affects some unknown processing of the component Browser Extension Provisioning. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216275.	5.0	More Details
CVE-2022-31708	vRealize Operations (vROps) contains a broken access control vulnerability. VMware has evaluated the severity of this issue to be in the Moderate severity range with a maximum CVSSv3 base score of 4.4.	4.9	More Details
CVE-2022-4108	The Wholesale Market for WooCommerce WordPress plugin before 1.0.8 does not validate user input used to generate system path, allowing high privilege users such as admin to download arbitrary file from the server even when they should not be able to (for example in multisite)	4.9	More Details
CVE-2022-20606	In SAEMM_MiningCodecTableWithMsgIE of SAEMM_RadioMessageCodec.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-233230674References: N/A	4.9	More Details
CVE-2022-46422	An issue in Netgear WNR2000 v1 1.2.3.7 and earlier allows authenticated attackers to cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process.	4.8	More Details
CVE-2022-4112	The Quizlord WordPress plugin through 2.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-3832	The External Media WordPress plugin before 1.0.36 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-40435	Employee Performance Evaluation System v1.0 was discovered to contain a persistent cross-site scripting (XSS) vulnerability via adding new entries under the Departments and Designations module.	4.8	More Details
CVE-2022-46430	TP-Link TL-WR740N V1 and V2 v3.12.4 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process.	4.8	More Details
CVE-2022-46428	TP-Link TL-WR1043ND V1 3.13.15 and earlier allows authenticated attackers to execute arbitrary code or cause a Denial of Service (DoS) via uploading a crafted firmware image during the firmware update process.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23527	mod_auth_openidc is an OpenID Certified™ authentication and authorization module for the Apache 2.x HTTP server. Versions prior to 2.4.12.2 are vulnerable to Open Redirect. When providing a logout parameter to the redirect URI, the existing code in oidc_validate_redirect_url() does not properly check for URLs that start with /\t, leading to an open redirect. This issue has been patched in version 2.4.12.2. Users unable to upgrade can mitigate the issue by configuring mod_auth_openidc to only allow redirection when the destination matches a given regular expression with OIDCRedirectURLsAllowed.	4.7	More Details
CVE-2020-36617	A vulnerability was found in ewxrjk sftpserver. It has been declared as problematic. Affected by this vulnerability is the function sftp_parse_path of the file parse.c. The manipulation leads to uninitialized pointer. The real existence of this vulnerability is still doubted at the moment. The name of the patch is bf4032f34832ee11d79aa60a226cc018e7ec5eed. It is recommended to apply a patch to fix this issue. The identifier VDB-216205 was assigned to this vulnerability. NOTE: In some deployment models this would be a vulnerability. README specifically warns about avoiding such deployment models.	4.6	More Details
CVE-2022-3917	Improper access control of bootloader function was discovered in Motorola Mobility Motorola e20 prior to version RONS31.267-38-8 allows attacker with local access to read partition or RAM data.	4.6	More Details
CVE-2022-46771	IBM UrbanCode Deploy (UCD) 6.2.0.0 through 6.2.7.18, 7.0.5.0 through 7.0.5.13, 7.1.0.0 through 7.1.2.9, 7.2.0.0 through 7.2.3.2 and 7.3.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 242273.	4.6	More Details
CVE-2022-4130	A blind site-to-site request forgery vulnerability was found in Satellite server. It is possible to trigger an external interaction to an attacker's server by modifying the Referer header in an HTTP request of specific resources in the server.	4.5	More Details
CVE-2022-20589	In valid_va_secbuf_check of drm_access_control.c, there is a possible ID due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-238841928References: N/A	4.4	More Details
CVE-2022-20555	In ufdt_get_node_by_path_len of ufdt_convert.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-246194233	4.4	More Details
CVE-2022-20544	In onOptionsItemSelected of ManageApplications.java, there is a possible bypass of profile owner restrictions 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-238745070	4.4	More Details
CVE-2022-20593	In pop_descriptor_string of BufferDescriptor.h, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239415809References: N/A	4.4	More Details
CVE-2022-42532	In Pixel firmware, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242332610References: N/A	4.4	More Details
CVE-2022-42515	In MiscService::DoOemSetRtpPktlossThreshold of miscservice.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241763503References: N/A	4.4	More Details
CVE-2022-42516	In ProtocolSimBuilderLegacy::BuildSimGetGbaAuth of protocolsimbuilderlegacy.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241763577References: N/A	4.4	More Details
CVE-2022-42512	In VsimOperationDataExt::encode of vsimdata.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241763050References: N/A	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42543	In fdt_path_offset_namelen of fdt_ro.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-249998113References: N/A	4.4	More Details
CVE-2022-39166	IBM Security Guardium 11.4 could allow a privileged user to obtain sensitive information inside of an HTTP response. IBM X-Force ID: 235405.	4.4	More Details
CVE-2022-42522	In DoSetCarrierConfig of miscservice.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-243130038References: N/A	4.4	More Details
CVE-2022-20595	In getWpcAuthChallengeResponse of WirelessCharger.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-239700137References: N/A	4.4	More Details
CVE-2022-42514	In ProtocolImsBuilder::BuildSetConfig of protocolimsbuilder.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241763298References: N/A	4.4	More Details
CVE-2022-42530	In Pixel firmware, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-242331893References: N/A	4.4	More Details
CVE-2022-42517	In MiscService::DoOemSetTcsFci of miscservice.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-241763682References: N/A	4.4	More Details
CVE-2022-32945	An access issue was addressed with additional sandbox restrictions on third-party apps. This issue is fixed in macOS Ventura 13. An app may be able to record audio with paired AirPods.	4.3	More Details
CVE-2022-38756	A vulnerability has been identified in Micro Focus GroupWise Web in versions prior to 18.4.2. The GW Web component makes a request to the Post Office Agent that contains sensitive information in the query parameters that could be logged by any intervening HTTP proxies.	4.3	More Details
CVE-2022-3876	A vulnerability, which was classified as problematic, has been found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. This issue affects some unknown processing of the file /api/browserextension/UpdatePassword/ of the component API. The manipulation of the argument PasswordID leads to authorization bypass. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The identifier VDB-216245 was assigned to this vulnerability.	4.3	More Details
CVE-2021-4249	A vulnerability was found in xml-conduit. It has been classified as problematic. Affected is an unknown function of the file xml-conduit/src/Text/XML/Stream/Parse.hs of the component DOCTYPE Entity Expansion Handler. The manipulation leads to infinite loop. It is possible to launch the attack remotely. Upgrading to version 1.9.1.0 is able to address this issue. The name of the patch is 4be1021791dcdee8b164d239433a2043dc0939ea. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216204.	4.3	More Details
CVE-2022-4604	A vulnerability classified as problematic was found in wp-english-wp-admin Plugin up to 1.5.1. Affected by this vulnerability is the function register_endpoints of the file english-wp-admin.php. The manipulation leads to cross-site request forgery. The attack can be launched remotely. Upgrading to version 1.5.2 is able to address this issue. The name of the patch is ad4ba171c974c65c3456e7c6228f59f40783b33d. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216199.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4603	A vulnerability classified as problematic has been found in ppp. Affected is the function dumpppp of the file pppdump/pppdump.c of the component pppdump. The manipulation of the argument spkt.buf/rpkt.buf leads to improper validation of array index. The real existence of this vulnerability is still doubted at the moment. The name of the patch is a75fb7b198eed50d769c80c36629f38346882cbf. It is recommended to apply a patch to fix this issue. VDB-216198 is the identifier assigned to this vulnerability. NOTE: pppdump is not used in normal process of setting up a PPP connection, is not installed setuid-root, and is not invoked automatically in any scenario.	4.3	More Details
CVE-2022-4612	A vulnerability has been found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome and classified as problematic. This vulnerability affects unknown code. The manipulation leads to insufficiently protected credentials. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. VDB-216274 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-4587	A vulnerability, which was classified as problematic, has been found in Opencaching Deutschland oc-server3. This issue affects some unknown processing of the file htdocs/templates2/ocstyle/login.tpl of the component Login Page. The manipulation of the argument username leads to cross site scripting. The attack may be initiated remotely. The name of the patch is 3296ebd61e7fe49e93b5755d5d7766d6e94a7667. It is recommended to apply a patch to fix this issue. The identifier VDB-216173 was assigned to this vulnerability.	4.3	More Details
CVE-2022-4611	A vulnerability, which was classified as problematic, was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. This affects an unknown part. The manipulation leads to hard-coded credentials. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The identifier VDB-216273 was assigned to this vulnerability.	4.3	More Details
CVE-2022-4565	A vulnerability classified as problematic was found in Dromara HuTool up to 5.8.10. This vulnerability affects unknown code of the file cn.hutool.core.util.ZipUtil.java. The manipulation leads to resource consumption. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 5.8.11 is able to address this issue. It is recommended to upgrade the affected component. VDB-215974 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-41960	BigBlueButton is an open source web conferencing system. Versions prior to 2.4.3, are subject to Insufficient Verification of Data Authenticity, resulting in Denial of Service. An attacker can make a Meteor call to `validateAuthToken` using a victim's userId, meetingId, and an invalid authToken. This forces the victim to leave the conference, because the resulting verification failure is also observed and handled by the victim's client. The attacker must be a participant in any meeting on the server. This issue is patched in version 2.4.3. There are no workarounds.	4.3	More Details
CVE-2022-41961	BigBlueButton is an open source web conferencing system. Versions prior to 2.4-rc-6 are subject to Ineffective user bans. The attacker could register multiple users, and join the meeting with one of them. When that user is banned, they could still join the meeting with the remaining registered users from the same extId. This issue has been fixed by improving permissions such that banning a user removes all users related to their extId, including registered users that have not joined the meeting. This issue is patched in versions 2.4-rc-6 and 2.5-alpha-1. There are no workarounds.	4.3	More Details
CVE-2022-4564	A vulnerability classified as problematic has been found in University of Central Florida Materia up to 9.0.0. This affects the function before of the file fuel/app/classes/controller/api.php of the component API Controller. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. Upgrading to version 9.0.1-alpha1 is able to address this issue. The name of the patch is af259115d2e8f17068e61902151ee8a9dbac397b. It is recommended to upgrade the affected component. The identifier VDB-215973 was assigned to this vulnerability.	4.3	More Details
CVE-2022-4124	The Popup Manager WordPress plugin through 1.6.6 does not have authorisation and CSRF checks when deleting popups, which could allow unauthenticated users to delete them	4.3	More Details
CVE-2022-42351	Adobe Experience Manager version 6.5.14 (and earlier) is affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to disclose low level confidentiality information. Exploitation of this issue does not require user interaction.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4125	The Popup Manager WordPress plugin through 1.6.6 does not have authorisation and CSRF check when creating/updating popups, and is missing sanitisation as well as escaping, which could allow unauthenticated attackers to create arbitrary popups and add Stored XSS payloads as well	4.3	More Details
CVE-2021-4247	A vulnerability has been found in OWASP NodeGoat and classified as problematic. This vulnerability affects unknown code of the file app/routes/research.js of the component Query Parameter Handler. The manipulation leads to denial of service. The attack can be initiated remotely. The name of the patch is 4a4d1db74c63fb4ff8d366551c3af006c25ead12. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216184.	4.3	More Details
CVE-2022-23490	BigBlueButton is an open source web conferencing system. Versions prior to 2.4.0 expose sensitive information to Unauthorized Actors. This issue affects meetings with polls, where the attacker is a meeting participant. Subscribing to the current-poll collection does not update the client UI, but does give the attacker access to the contents of the collection, which include the individual poll responses. This issue is patched in version 2.4.0. There are no workarounds.	4.3	More Details
CVE-2022-20541	In phNxpNciHal_ioctl of phNxpNciHal.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-238083126	4.2	More Details
CVE-2021-4258	A vulnerability was found in whohas. It has been rated as problematic. This issue affects some unknown processing of the component Package Information Handler. The manipulation leads to cleartext transmission of sensitive information. The attack may be initiated remotely. The real existence of this vulnerability is still doubted at the moment. The name of the patch is 667c3e2e9178f15c23d7918b5db25cd0792c8472. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216251. NOTE: Most sources redirect to the encrypted site which limits the possibilities of an attack.	3.7	More Details
CVE-2022-44488	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction.	3.5	More Details
CVE-2022-4602	A vulnerability was found in Shoplazza LifeStyle 1.1. It has been rated as problematic. This issue affects some unknown processing of the file /admin/api/theme-edit/ of the component Review Flow Handler. The manipulation of the argument Title 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-216197 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4558	A vulnerability was found in Alinto SOGo up to 5.7.1. It has been classified as problematic. This affects an unknown part of the file SoObjects/SOGo/NSString+Utilities.m of the component Folder/Mail Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 5.8.0 is able to address this issue. The name of the patch is 1e0f5f00890f751e84d67be4f139dd7f00faa5f3. It is recommended to upgrade the affected component. The identifier VDB-215961 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4556	A vulnerability was found in Alinto SOGo up to 5.7.1 and classified as problematic. Affected by this issue is the function _migrateMailIdentities of the file SoObjects/SOGo/SOGoUserDefaults.m of the component Identity Handler. The manipulation of the argument fullName leads to cross site scripting. The attack may be launched remotely. Upgrading to version 5.8.0 is able to address this issue. The name of the patch is efac49ae91a4a325df9931e78e543f707a0f8e5e. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-215960.	3.5	More Details
CVE-2022-4593	A vulnerability was found in retra-system. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is a6d94ab88f4a6f631a14c59b72461140fb57ae1f. It is recommended to apply a patch to fix this issue. VDB-216186 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4595	A vulnerability classified as problematic has been found in django-openipam. This affects an unknown part of the file openipam/report/templates/report/exposed_hosts.html. The manipulation of the argument description leads to cross site scripting. It is possible to initiate the attack remotely. The name of the patch is a6223a1150d60cd036106ba6a8e676c1bfc3cc85. It is recommended to apply a patch to fix this issue. The identifier VDB-216189 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4596	A vulnerability, which was classified as problematic, has been found in Shoplazza 1.1. This issue affects some unknown processing of the file /admin/api/admin/articles/ of the component Add Blog Post Handler. The manipulation of the argument Title leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-216191.	3.5	More Details
CVE-2022-4597	A vulnerability, which was classified as problematic, was found in Shoplazza LifeStyle 1.1. Affected is an unknown function of the file /admin/api/admin/v2_products of the component Create Product Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-216192.	3.5	More Details
CVE-2022-4598	A vulnerability has been found in Shoplazza LifeStyle 1.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/api/theme-edit/ of the component Announcement Handler. The manipulation of the argument Text/Mobile Text 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-216193 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4599	A vulnerability was found in Shoplazza LifeStyle 1.1 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/api/theme-edit/ of the component Product Handler. The manipulation of the argument Subheading/Heading/Text/Button Text/Label leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-216194 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4600	A vulnerability was found in Shoplazza LifeStyle 1.1. It has been classified as problematic. This affects an unknown part of the file /admin/api/theme-edit/ of the component Product Carousel Handler. The manipulation of the argument Heading/Description 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-216195.	3.5	More Details
CVE-2022-4601	A vulnerability was found in Shoplazza LifeStyle 1.1. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/api/theme-edit/ of the component Shipping/Member Discount/Icon. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-216196.	3.5	More Details
CVE-2021-4250	A vulnerability classified as problematic has been found in cgriego active_attr up to 0.15.2. This affects the function call of the file lib/active_attr/typecasting/boolean_typecaster.rb of the component Regex Handler. The manipulation of the argument value leads to denial of service. The exploit has been disclosed to the public and may be used. Upgrading to version 0.15.3 is able to address this issue. The name of the patch is dab95e5843b01525444b82bd7b336ef1d79377df. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216207.	3.5	More Details
CVE-2022-4560	A vulnerability was found in Joget up to 7.0.31. It has been rated as problematic. This issue affects the function getInternalJsCssLib of the file wflow-core/src/main/java/org/joget/plugin/enterprise/UniversalTheme.java of the component wflow-core. The manipulation of the argument key leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 7.0.32 is able to address this issue. The name of the patch is ecf8be8f6f0cb725c18536ddc726d42a11bdaa1b. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-215963.	3.5	More Details
CVE-2021-4251	A vulnerability classified as problematic was found in as. This vulnerability affects the function getFullURL of the file include.cdn.php. The manipulation leads to cross site scripting. The attack can be initiated remotely. The name of the patch is 4acad1e3d2c34c017473ceea442fb3e3e078b2bd. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216208.	3.5	More Details
CVE-2022-4495	A vulnerability, which was classified as problematic, has been found in collective.dms.basecontent up to 1.6. This issue affects the function renderCell of the file src/collective/dms/basecontent/browser/column.py. The manipulation leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 1.7 is able to address this issue. The name of the patch is 6c4d616fcc771822a14ebae5e23f3f6d96d134bd. It is recommended to upgrade the affected component. The identifier VDB-215813 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4252	A vulnerability, which was classified as problematic, has been found in WP-Ban. This issue affects the function toggle_checkbox of the file ban-options.php. The manipulation of the argument $_SERVER["HTTP_USER_AGENT"] leads to cross site scripting. The attack may be initiated remotely. The name of the patch is 13e0b1e922f3aaa3f8fcb1dd6d50200dd693fd76. It is recommended to apply a patch to fix this issue. The identifier VDB-216209 was assigned to this vulnerability.	3.5	More Details
CVE-2021-4253	A vulnerability, which was classified as problematic, was found in ctrlo lenio. Affected is an unknown function in the library lib/Lenio.pm of the component Ticket Handler. The manipulation of the argument site_id leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is 7a1f90bd2a0ce95b8338ec0926902da975ec64d9. It is recommended to apply a patch to fix this issue. VDB-216210 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2021-4254	A vulnerability has been found in ctrlo lenio and classified as problematic. Affected by this vulnerability is an unknown functionality of the file views/layouts/main.tt of the component Notice Handler. The manipulation of the argument notice.notice.text leads to cross site scripting. The attack can be launched remotely. The name of the patch is aa300555343c1c081951fcb68bfb6852fbba7451. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216211.	3.5	More Details
CVE-2021-4255	A vulnerability was found in ctrlo lenio and classified as problematic. Affected by this issue is some unknown functionality of the file views/contractor.tt. The manipulation of the argument contractor.name leads to cross site scripting. The attack may be launched remotely. The name of the patch is e1646d5cd0a2fbab9eb505196dd2ca1c9e4cdd97. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216212.	3.5	More Details
CVE-2021-4256	A vulnerability was found in ctrlo lenio. It has been classified as problematic. This affects an unknown part of the file views/index.tt. The manipulation of the argument task.name/task.site.org.name leads to cross site scripting. It is possible to initiate the attack remotely. The name of the patch is e1646d5cd0a2fbab9eb505196dd2ca1c9e4cdd97. It is recommended to apply a patch to fix this issue. The identifier VDB-216213 was assigned to this vulnerability.	3.5	More Details
CVE-2022-3877	A vulnerability, which was classified as problematic, was found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. Affected is an unknown function of the component URL Field Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. VDB-216246 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2021-4257	A vulnerability was found in ctrlo lenio. It has been declared as problematic. This vulnerability affects unknown code of the file views/task.tt of the component Task Handler. The manipulation of the argument site.org.name/check.name/task.tasktype.name/task.name leads to cross site scripting. The attack can be initiated remotely. The name of the patch is 698c5fa465169d6f23c6a41ca4b1fc9a7869013a. It is recommended to apply a patch to fix this issue. VDB-216214 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4559	A vulnerability was found in INEX IPX-Manager up to 6.2.0. It has been declared as problematic. This vulnerability affects unknown code of the file resources/views/customer/list.foil.php. The manipulation leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 6.3.0 is able to address this issue. The name of the patch is bc9b14c6f70cccdb89b559e8bc3a7318bfe9c243. It is recommended to upgrade the affected component. VDB-215962 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4525	A vulnerability has been found in National Sleep Research Resource sleepdata.org up to 58.x and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 59.0.0.rc is able to address this issue. The name of the patch is da44a3893b407087829b006d09339780919714cd. It is recommended to upgrade the affected component. The identifier VDB-215905 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4561	A vulnerability classified as problematic has been found in SemanticDrilldown Extension. Affected is the function printFilterLine of the file includes/specials/SDBrowseDataPage.php of the component GET Parameter Handler. The manipulation of the argument value leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is 6e18cf740a4548166c1d95f6d3a28541d298a3aa. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-215964.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4524	A vulnerability, which was classified as problematic, was found in Roots soil Plugin up to 4.0.x. Affected is the function language_attributes of the file src/Modules/CleanUpModule.php. The manipulation of the argument language leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 4.1.0 is able to address this issue. The name of the patch is 0c9151e00ab047da253e5cdbfccb204dd423269d. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-215904.	3.5	More Details
CVE-2022-4522	A vulnerability classified as problematic was found in CalendarXP up to 10.0.1. This vulnerability affects unknown code. The manipulation leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 10.0.2 is able to address this issue. The name of the patch is e3715b2228ddefe00113296069969f9e184836da. It is recommended to upgrade the affected component. VDB-215902 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4520	A vulnerability was found in WSO2 carbon-registry up to 4.8.11. It has been rated as problematic. Affected by this issue is some unknown functionality of the file components/registry/org.wso2.carbon.registry.search.ui/src/main/resources/web/search/advancedSearchForm-ajaxprocessor.jsp of the component Advanced Search. The manipulation of the argument mediaType/rightOp/leftOp/rightPropertyValue/leftPropertyValue leads to cross site scripting. The attack may be launched remotely. Upgrading to version 4.8.12 is able to address this issue. The name of the patch is 0c827cc1b14b82d8eb86117ab2e43c34bb91ddb4. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-215900.	3.5	More Details
CVE-2022-4585	A vulnerability classified as problematic has been found in Opencaching Deutschland oc-server3. This affects an unknown part of the file htdocs/templates2/ocstyle/start.tpl of the component Cookie Handler. The manipulation of the argument usercountryCode leads to cross site scripting. It is possible to initiate the attack remotely. The name of the patch is c720f2777a452186c67ef30db3679dd409556544. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216171.	3.5	More Details
CVE-2022-4586	A vulnerability classified as problematic was found in Opencaching Deutschland oc-server3. This vulnerability affects unknown code of the file htdocs/templates2/ocstyle/cachelists.tpl of the component Cachelist Handler. The manipulation of the argument name_filter/by_filter leads to cross site scripting. The attack can be initiated remotely. The name of the patch is a9f79c7da78cd24a7ef1d298e6bc86006972ea73. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216172.	3.5	More Details
CVE-2022-4523	A vulnerability, which was classified as problematic, has been found in vexim2. This issue affects some unknown processing. The manipulation leads to cross site scripting. The attack may be initiated remotely. The name of the patch is 21c0a60d12e9d587f905cd084b2c70f9b1592065. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-215903.	3.5	More Details
CVE-2022-4514	A vulnerability, which was classified as problematic, was found in Opencaching Deutschland oc-server3. Affected is an unknown function of the file htdocs/lang/de/ocstyle/varset.inc.php. The manipulation of the argument varvalue leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 4bdd6a0e7b7760cea03b91812cbb80d7b16e3b5f. It is recommended to apply a patch to fix this issue. VDB-215886 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4513	A vulnerability, which was classified as problematic, has been found in European Environment Agency eionet.contreg. This issue affects some unknown processing. The manipulation of the argument searchTag/resourceUri leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 2022-06-27T0948 is able to address this issue. The name of the patch is a120c2153e263e62c4db34a06ab96a9f1c6bccb6. It is recommended to upgrade the affected component. The identifier VDB-215885 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4521	A vulnerability classified as problematic has been found in WSO2 carbon-registry up to 4.8.6. This affects an unknown part of the component Request Parameter Handler. The manipulation of the argument parentPath/path/username/path/profile_menu leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 4.8.7 is able to address this issue. The name of the patch is 9f967abfde9317bee2cda469dbc09b57d539f2cc. It is recommended to upgrade the affected component. The identifier VDB-215901 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4590	A vulnerability was found in mschaef toto up to 1.4.20. It has been classified as problematic. This affects an unknown part of the component Todo List Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 1.4.21 is able to address this issue. The name of the patch is fdc825ac5249f40683377e8a526a06cdc6870125. It is recommended to upgrade the affected component. The identifier VDB-216177 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4591	A vulnerability was found in mschaef toto up to 1.4.20. It has been declared as problematic. This vulnerability affects unknown code of the component Email Parameter Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 1.4.21 is able to address this issue. The name of the patch is 1f27f37c1a06f54a76971f70eaa6139dc139bdf9. It is recommended to upgrade the affected component. VDB-216178 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4582	A vulnerability was found in starter-public-edition-4 up to 4.6.10. It has been classified as problematic. Affected is an unknown function. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 4.6.11 is able to address this issue. The name of the patch is 2606983c20f6ea3430ac4b36b3d2e88aafef45da. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216168.	3.5	More Details
CVE-2022-4526	A vulnerability was found in django-photologue up to 3.15.1 and classified as problematic. Affected by this issue is some unknown functionality of the file photologue/templates/photologue/photo_detail.html of the component Default Template Handler. The manipulation of the argument object.caption leads to cross site scripting. The attack may be launched remotely. Upgrading to version 3.16 is able to address this issue. The name of the patch is 960cb060ce5e2964e6d716ff787c72fc18a371e7. It is recommended to apply a patch to fix this issue. VDB-215906 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4527	A vulnerability was found in collective.task up to 3.0.8. It has been classified as problematic. This affects the function renderCell/AssignedGroupColumn of the file src/collective/task/browser/table.py. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 3.0.9 is able to address this issue. The name of the patch is 1aac7f83fa2c2b41d59ba02748912953461f3fac. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-215907.	3.5	More Details
CVE-2022-4581	A vulnerability was found in 1j01 mind-map and classified as problematic. This issue affects some unknown processing of the file app.coffee. The manipulation of the argument html leads to cross site scripting. The attack may be initiated remotely. The name of the patch is 9617e6084dfeccd92079ab4d7f439300a4b24394. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216167.	3.5	More Details
CVE-2022-20519	In onCreate of AddAppNetworksActivity.java, there is a possible way for a guest user to configure WiFi networks 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-224772678	3.3	More Details
CVE-2022-20537	In createDialog of WifiScanModeActivity.java, there is a possible way for a Guest user to enable location-sensitive settings due to 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-13Android ID: A-235601169	3.3	More Details
CVE-2022-20525	In enforceVisualVoicemailPackage of PhoneInterfaceManager.java, there is a possible leak of visual voicemail package name 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-229742768	3.3	More Details
CVE-2022-20528	In findParam of HevcUtils.cpp there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-230172711	3.3	More Details
CVE-2022-20558	In registerReceivers of DeviceCapabilityListener.java, there is a possible way to change preferred TTY mode 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-236264289	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20526	In CanvasContext::draw of CanvasContext.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-229742774	3.3	More Details
CVE-2022-20562	In various functions of ap_input_processor.c, there is a possible way to record audio during a phone call due to a logic error in the code. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-231630423References: N/A	3.3	More Details
CVE-2022-20533	In getSlice of WifiSlice.java, there is a possible way to connect a new WiFi network from the guest mode 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-232798363	3.3	More Details
CVE-2022-20559	In revokeOwnPermissionsOnKill of PermissionManager.java, 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-219739967	3.3	More Details
CVE-2022-20535	In registerLocalOnlyHotspotSoftApCallback of WifiManager.java, 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-233605242	3.3	More Details
CVE-2022-20536	In registerBroadcastReceiver of RcsService.java, there is a possible way to change preferred TTY mode 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-235100180	3.3	More Details
CVE-2022-20556	In launchConfigNewNetworkFragment of NetworkProviderSettings.java, there is a possible way for the guest user to add a new WiFi network 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-246301667	3.3	More Details
CVE-2022-2966	Out-of-bounds Read vulnerability in Delta Electronics DOPSoft.This issue affects DOPSoft: All Versions.	3.3	More Details
CVE-2022-41972	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. Versions prior to 4.9 contain a NULL Pointer Dereference in BLE L2CAP module. The Contiki-NG operating system for IoT devices contains a Bluetooth Low Energy stack. An attacker can inject a packet in this stack, which causes the implementation to dereference a NULL pointer and triggers undefined behavior. More specifically, while processing the L2CAP protocol, the implementation maps an incoming channel ID to its metadata structure. In this structure, state information regarding credits is managed through calls to the function input_l2cap_credit in the module os/net/mac/ble/ble-l2cap.c. Unfortunately, the input_l2cap_credit function does not check that the metadata corresponding to the user-supplied channel ID actually exists, which can lead to the channel variable being set to NULL before a pointer dereferencing operation is performed. The vulnerability has been patched in the "develop" branch of Contiki-NG, and will be included in release 4.9. Users can apply the patch in Contiki-NG pull request #2253 as a workaround until the new package is released.	2.9	More Details
CVE-2022-41962	BigBlueButton is an open source web conferencing system. Versions prior to 2.4-rc-6, and 2.5-alpha-1 contain Incorrect Authorization for setting emoji status. A user with moderator rights can use the clear status feature to set any emoji status for other users. Moderators should only be able to set none as the status of other users. This issue is patched in 2.4-rc-6 and 2.5-alpha-1There are no workarounds.	2.7	More Details
CVE-2022-41963	BigBlueButton is an open source web conferencing system. Versions prior to 2.4.3 contain a whiteboard grace period that exists to handle delayed messages, but this grace period could be used by attackers to take actions in the few seconds after their access is revoked. The attacker must be a meeting participant. This issue is patched in version 2.4.3 an version 2.5-alpha-1	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20529	In multiple locations of WifiDialogActivity.java, there is a possible limited lockscreen bypass due to a logic error in the code. This could lead to local escalation of privilege in wifi settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-231583603	2.4	More Details
CVE-2022-4588	A vulnerability, which was classified as problematic, was found in Boston Sleep slice up to 84.1.x. Affected is an unknown function of the component Layout Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 84.2.0 is able to address this issue. The name of the patch is 6523bb17d889e2ab13d767f38afefdb37083f1d0. It is recommended to upgrade the affected component. VDB-216174 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2022-20543	In multiple locations, there is a possible display crash loop due to improper input validation. This could lead to local denial of service with system execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-238178261	2.3	More Details
CVE-2022-38653	In HCL Digital Experience, customized XSS payload can be constructed such that it is served in the application unencoded.	2.0	More Details
CVE-2022-4610	A vulnerability, which was classified as problematic, has been found in Click Studios Passwordstate and Passwordstate Browser Extension Chrome. Affected by this issue is some unknown functionality. The manipulation leads to risky cryptographic algorithm. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-216272.	1.9	More Details
CVE-2022-39925	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-2022-39920	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-2022-39921	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-2022-39922	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-2022-39918	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-2022-39923	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-2022-39917	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-2022-39916	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-2022-39924	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-2022-39919	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-2022-39933	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-2022-39926	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-2022-39927	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-2022-39943	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-2022-39942	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-2022-39940	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-2022-39939	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-2022-39938	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-2022-39937	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-2022-39936	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-2022-4579	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-2022-39935	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-2022-39934	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-2022-39932	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-2022-39931	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-2022-39930	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-2022-39929	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-2022-39928	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-2022-39941	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