SingCERT

Singapore Cyber Emergency Response Team

Security Bulletin 26 October 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-27624	A vulnerability regarding improper restriction of operations within the bounds of a memory buffer is found in the packet decryption functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500.	10.0	More Details
CVE-2022-33192	Four OS command injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these vulnerabilities.This vulnerability specifically focuses on the unsafe use of the `WL_SSID` and `WL_SSID_HEX` configuration values in the function at offset `0x1c7d28` of firmware 6.9Z.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33194	Four OS command injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the `WL_Key` and `WL_DefaultKeyID` configuration values in the function located at offset `0x1c7d28` of firmware 6.9Z , and even more specifically on the command execution occuring at offset `0x1c7f6c`.	10.0	More Details
CVE-2022-33195	Four OS command injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the `WL_DefaultKeyID` in the function located at offset `0x1c7d28` of firmware 6.9Z, and even more specifically on the command execution occuring at offset `0x1c7fac`.	10.0	More Details
CVE-2022-27626	A vulnerability regarding concurrent execution using shared resource with improper synchronization ('Race Condition') is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500.	10.0	More Details
CVE-2022-27625	A vulnerability regarding improper restriction of operations within the bounds of a memory buffer is found in the message processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to execute arbitrary commands via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500.	10.0	More Details
CVE-2021-26727	Multiple command injections and stack-based buffer overflows vulnerabilities in the SubNet_handler_func function of spx_restservice allow an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	10.0	More Details
CVE-2021-26728	Command injection and stack-based buffer overflow vulnerabilities in the KillDupUsr_func function of spx_restservice allow an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26729	Command injection and multiple stack-based buffer overflows vulnerabilities in the Login_handler_func function of spx_restservice allow an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	10.0	More Details
CVE-2021-26730	A stack-based buffer overflow vulnerability in a subfunction of the Login_handler_func function of spx_restservice allows an attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	10.0	More Details
CVE-2022-33193	Four OS command injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A XCMD can lead to arbitrary command execution. An attacker can send a sequence of malicious commands to trigger these vulnerabilities.This vulnerability specifically focuses on the unsafe use of the `WL_WPAPSK` configuration value in the function located at offset `0x1c7d28` of firmware 6.9Z.	10.0	More Details
CVE-2022-43405	A sandbox bypass vulnerability in Jenkins Pipeline: Groovy Libraries Plugin 612.v84da_9c54906d and earlier allows attackers with permission to define untrusted Pipeline libraries and to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM.	9.9	More Details
CVE-2022-43401	A sandbox bypass vulnerability involving various casts performed implicitly by the Groovy language runtime in Jenkins Script Security Plugin 1183.v774b_0b_0a_a_451 and earlier allows attackers with permission to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM.	9.9	More Details
CVE-2022-33204	Four OS command injection vulnerabilities exists in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the `ssid_hex` HTTP parameter to construct an OS Command at offset `0x19afc0` of the `/root/hpgw` binary included in firmware 6.9Z.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33205	Four OS command injection vulnerabilities exists in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the \`wpapsk_hex\` HTTP parameter to construct an OS Command at offset \`0x19b0ac\` of the \`/root/hpgw\` binary included in firmware 6.9Z.	9.9	More Details
CVE-2022-43406	A sandbox bypass vulnerability in Jenkins Pipeline: Deprecated Groovy Libraries Plugin 583.vf3b_454e43966 and earlier allows attackers with permission to define untrusted Pipeline libraries and to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM.	9.9	More Details
CVE-2022-33207	Four OS command injection vulnerabilities exists in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on a second unsafe use of the \`default_key_id\` HTTP parameter to construct an OS Command at offset \`0x19B234\` of the \`/root/hpgw\` binary included in firmware 6.9Z.	9.9	More Details
CVE-2022-33206	Four OS command injection vulnerabilities exists in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability focuses on the unsafe use of the \`key\` and \`default_key_id\` HTTP parameters to construct an OS Command crafted at offset \`0x19b1f4\` of the \`/root/hpgw\` binary included in firmware 6.9Z.	9.9	More Details
CVE-2022-43402	A sandbox bypass vulnerability involving various casts performed implicitly by the Groovy language runtime in Jenkins Pipeline: Groovy Plugin 2802.v5ea_628154b_c2 and earlier allows attackers with permission to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM.	9.9	More Details
CVE-2022-43403	A sandbox bypass vulnerability involving casting an array-like value to an array type in Jenkins Script Security Plugin 1183.v774b_0b_0a_a_451 and earlier allows attackers with permission to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43404	A sandbox bypass vulnerability involving crafted constructor bodies and calls to sandbox-generated synthetic constructors in Jenkins Script Security Plugin 1183.v774b_0b_0a_a_451 and earlier allows attackers with permission to define and run sandboxed scripts, including Pipelines, to bypass the sandbox protection and execute arbitrary code in the context of the Jenkins controller JVM.	9.9	More Details
CVE-2022-32765	An OS command injection vulnerability exists in the sysupgrade command injection functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	9.8	More Details
CVE-2022-33189	An OS command injection vulnerability exists in the XCMD setAlexa functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send a malicious XML payload to trigger this vulnerability.	9.8	More Details
CVE-2022-32454	A stack-based buffer overflow vulnerability exists in the XCMD setIPCam functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to remote code execution. An attacker can send a malicious XML payload to trigger this vulnerability.	9.8	More Details
CVE-2022-30541	An OS command injection vulnerability exists in the XCMD setUPnP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send a malicious XML payload to trigger this vulnerability.	9.8	More Details
CVE-2022-32773	An OS command injection vulnerability exists in the XCMD doDebug functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send a malicious XML payload to trigger this vulnerability.	9.8	More Details
CVE-2022-29889	A hard-coded password vulnerability exists in the telnet functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z. Use of a hard-coded root password can lead to arbitrary command execution. An attacker can authenticate with hard-coded credentials to trigger this vulnerability.	9.8	More Details
CVE-2022-29851	documentconverter in OX App Suite through 7.10.6, in a non-default configuration with ghostscript, allows OS Command Injection because file conversion may occur for an EPS document that is disguised as a PDF document.	9.8	More Details
CVE-2022-33150	An OS command injection vulnerability exists in the js_package install functionality of Robustel R1510 3.1.16. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-20016	MVPower CCTV DVR models, including TV-7104HE 1.8.4 115215B9 and TV7108HE, contain a web shell that is accessible via a /shell URI. A remote unauthenticated attacker can execute arbitrary operating system commands as root. This vulnerability has also been referred to as the "JAWS webserver RCE" because of the easily identifying HTTP response server field. Other firmware versions, at least from 2014 through 2019, can be affected. This was exploited in the wild in 2017 through 2022.	9.8	More Details
CVE-2022-29477	An authentication bypass vulnerability exists in the web interface /action/factory* functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP header can lead to authentication bypass. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2022-33938	A format string injection vulnerability exists in the ghome_process_control_packet functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted XCMD can lead to memory corruption, information disclosure and denial of service. An attacker can send a malicious XML payload to trigger this vulnerability.	9.8	More Details
CVE-2022-35244	A format string injection vulnerability exists in the XCMD getVarHA functionality of abode systems, inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to memory corruption, information disclosure, and denial of service. An attacker can send a malicious XML payload to trigger this vulnerability.	9.8	More Details
CVE-2022-35874	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This vulnerability arises from format string injection via the \`ssid\` and \`ssid_hex\` configuration parameters, as used within the \`testWifiAP\` XCMD handler	9.8	More Details
CVE-2022-35875	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This vulnerability arises from format string injection via the \`wpapsk\` configuration parameter, as used within the \`testWifiAP\` XCMD handler	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35876	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This vulnerability arises from format string injection via the \`default_key_id\` and \`key\` configuration parameters, as used within the \`testWifiAP\` XCMD handler	9.8	More Details
CVE-2022-35877	Four format string injection vulnerabilities exist in the XCMD testWifiAP functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. Specially-crafted configuration values can lead to memory corruption, information disclosure and denial of service. An attacker can modify a configuration value and then execute an XCMD to trigger these vulnerabilities.This vulnerability arises from format string injection via the \`default_key_id\` configuration parameter, as used within the \`testWifiAP\` XCMD handler	9.8	More Details
CVE-2022-38580	Zalando Skipper v0.13.236 is vulnerable to Server-Side Request Forgery (SSRF).	9.8	More Details
CVE-2022-39312	Dataease is an open source data visualization analysis tool. Dataease prior to 1.15.2 has a deserialization vulnerability. In Dataease, the Mysql data source in the data source function can customize the JDBC connection parameters and the Mysql server target to be connected. In \`backend/src/main/java/io/dataease/provider/datasource/JdbcProvider.java\`, the \`MysqlConfiguration\` class does not filter any parameters. If an attacker adds some parameters to a JDBC url and connects to a malicious mysql server, the attacker can trigger the mysql jdbc deserialization vulnerability. Through the deserialization vulnerability, the attacker can execute system commands and obtain server privileges. Version 1.15.2 contains a patch for this issue.	9.8	More Details
CVE-2022-39345	Gin-vue-admin is a backstage management system based on vue and gin, which separates the front and rear of the full stack. Gin-vue-admin prior to 2.5.4 is vulnerable to path traversal, which leads to file upload vulnerabilities. Version 2.5.4 contains a patch for this issue. There are no workarounds aside from upgrading to a patched version.	9.8	More Details
CVE-2022-3393	The Post to CSV by BestWebSoft WordPress plugin through 1.4.0 does not properly escape fields when exporting data as CSV, leading to a CSV injection	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36452	A vulnerability in the web conferencing component of Mitel MiCollab through 9.5.0.101 could allow an unauthenticated attacker to upload malicious files. A successful exploit could allow an attacker to execute arbitrary code within the context of the application.	9.8	More Details
CVE-2022-29520	An OS command injection vulnerability exists in the console_main_loop :sys functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z. A specially-crafted XCMD can lead to arbitrary command execution. An attacker can send an XML payload to trigger this vulnerability.	9.8	More Details
CVE-2022-41711	Badaso version 2.6.0 allows an unauthenticated remote attacker to execute arbitrary code remotely on the server. This is possible because the application does not properly validate the data uploaded by users.	9.8	More Details
CVE-2022-29472	An OS command injection vulnerability exists in the web interface util_set_serial_mac functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2022-37298	Shinken Solutions Shinken Monitoring Version 2.4.3 affected is vulnerable to Incorrect Access Control. The SafeUnpickler class found in shinken/safepickle.py implements a weak authentication scheme when unserializing objects passed from monitoring nodes to the Shinken monitoring server.	9.8	More Details
CVE-2022-25720	Memory corruption in WLAN due to out of bound array access during connect/roaming in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	9.8	More Details
CVE-2022-25748	Memory corruption in WLAN due to integer overflow to buffer overflow while parsing GTK frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.8	More Details
CVE-2022-41415	Acer Altos W2000h-W570h F4 R01.03.0018 was discovered to contain a stack overflow in the RevserveMem component. This vulnerability allows attackers to cause a Denial of Service (DoS) via injecting crafted shellcode into the NVRAM variable.	9.8	More Details
CVE-2022-43184	D-Link DIR878 1.30B08 Hotfix_04 was discovered to contain a command injection vulnerability via the component /bin/proc.cgi.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43019	OpenCATS v0.9.6 was discovered to contain a remote code execution (RCE) vulnerability via the getDataGridPager's ajax functionality.	9.8	More Details
CVE-2022-43024	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the list parameter at /goform/SetVirtualServerCfg.	9.8	More Details
CVE-2022-43025	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the startIp parameter at /goform/SetPptpServerCfg.	9.8	More Details
CVE-2022-43026	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the endIp parameter at /goform/SetPptpServerCfg.	9.8	More Details
CVE-2022-43027	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the firewallEn parameter at /goform/SetFirewallCfg.	9.8	More Details
CVE-2022-43028	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the timeZone parameter at /goform/SetSysTimeCfg.	9.8	More Details
CVE-2022-43029	Tenda TX3 US_TX3V1.0br_V16.03.13.11_multi_TDE01 was discovered to contain a stack overflow via the time parameter at /goform/SetSysTimeCfg.	9.8	More Details
CVE-2022-27805	An authentication bypass vulnerability exists in the GHOME control functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted network request can lead to arbitrary XCMD execution. An attacker can send a malicious XML payload to trigger this vulnerability.	9.8	More Details
CVE-2022-3327	Missing Authentication for Critical Function in GitHub repository ikus060/rdiffweb prior to 2.5.0a6.	9.8	More Details
CVE-2022-37598	Prototype pollution vulnerability in function DEFNODE in ast.js in mishoo UglifyJS 3.13.2 via the name variable in ast.js. NOTE: the vendor considers this an invalid report.	9.8	More Details
CVE-2022-42021	Best Student Result Management System v1.0 is vulnerable to SQL Injection via /upresult/upresult/notice-details.php?nid=.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42233	Tenda 11N with firmware version V5.07.33_cn suffers from an Authentication Bypass vulnerability.	9.8	More Details
CVE-2022-37454	The Keccak XKCP SHA-3 reference implementation before fdc6fef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface.	9.8	More Details
CVE-2022-3203	On ORing net IAP-420(+) with FW version 2.0m a telnet server is enabled by default and cannot permanently be disabled. You can connect to the device via LAN or WiFi with hardcoded credentials and get an administrative shell. These credentials are reset to defaults with every reboot.	9.8	More Details
CVE-2022-43400	A vulnerability has been identified in Siveillance Video Mobile Server V2022 R2 (All versions < V22.2a (80)). The mobile server component of affected applications improperly handles the log in for Active Directory accounts that are part of Administrators group. This could allow an unauthenticated remote attacker to access the application without a valid account.	9.8	More Details
CVE-2021-42010	Heron versions <= 0.20.4-incubating allows CRLF log injection because of the lack of escaping in the log statements. Please update to version 0.20.5-incubating which addresses this issue.	9.8	More Details
CVE-2016-20017	D-Link DSL-2750B devices before 1.05 allow remote unauthenticated command injection via the login.cgi cli parameter, as exploited in the wild in 2016 through 2022.	9.8	More Details
CVE-2022-39305	Gin-vue-admin is a backstage management system based on vue and gin, which separates the front and rear of the full stack. Versions prior to 2.5.4 contain a file upload ability. The affected code fails to validate fileMd5 and fileName parameters, resulting in an arbitrary file being read. This issue is patched in 2.5.4b. There are no known workarounds.	9.8	More Details
CVE-2022-40984	Stack-based buffer overflow in WTViewerE series WTViewerE 761941 from 1.31 to 1.61 and WTViewerEfree from 1.01 to 1.52 allows an attacker to cause the product to crash by processing a long file name.	9.8	More Details
CVE-2022-27804	An os command injection vulnerability exists in the web interface util_set_abode_code functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can send an HTTP request to trigger this vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33897	A directory traversal vulnerability exists in the web_server /ajax/remove/ functionality of Robustel R1510 3.1.16. A specially-crafted network request can lead to arbitrary file deletion. An attacker can send a sequence of requests to trigger this vulnerability.	9.1	More Details
CVE-2021-26731	Command injection and multiple stack-based buffer overflows vulnerabilities in the modifyUserb_func function of spx_restservice allow an authenticated attacker to execute arbitrary code with the same privileges as the server user (root). This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	9.1	More Details
CVE-2022-39322	@keystone-6/core is a core package for Keystone 6, a content management system for Node.js. Starting with version 2.2.0 and prior to version 2.3.1, users who expected their `multiselect` fields to use the field-level access control - if configured - are vulnerable to their field-level access control not being used. List-level access control is not affected. Field-level access control for fields other than `multiselect` are not affected. Version 2.3.1 contains a fix for this issue. As a workaround, stop using the `multiselect` field.	9.1	More Details
CVE-2022-25718	Cryptographic issue in WLAN due to improper check on return value while authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	9.1	More Details
CVE-2021-46848	GNU Libtasn1 before 4.19.0 has an ETYPE_OK off-by-one array size check that affects asn1_encode_simple_der.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-35878	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted UPnP negotiation can lead to memory corruption, information disclosure, and denial of service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `ST` and `Location` HTTP response headers, as used within the `DoEnumUPnPService` action handler.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39321	GitHub Actions Runner is the application that runs a job from a GitHub Actions workflow. The actions runner invokes the docker cli directly in order to run job containers, service containers, or container actions. A bug in the logic for how the environment is encoded into these docker commands was discovered in versions prior to 2.296.2, 2.293.1, 2.289.4, 2.285.2, and 2.283.4 that allows an input to escape the environment variable and modify that docker command invocation directly. Jobs that use container actions, job containers, or service containers alongside untrusted user inputs in environment variables may be vulnerable. The Actions Runner has been patched, both on `github.com` and hotfixes for GHES and GHAE customers in versions 2.296.2, 2.293.1, 2.289.4, 2.285.2, and 2.283.4. GHES and GHAE customers may want to patch their instance in order to have their runners automatically upgrade to these new runner versions. As a workaround, users may consider removing any container actions, job containers, or service containers from their jobs until they are able to upgrade their runner versions.	8.8	More Details
CVE-2022-35887	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from format string injection via the `default_key_id` HTTP parameter, as used within the `/action/wirelessConnect` handler.	8.8	More Details
CVE-2022-35886	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from format string injection via the `default_key_id` and `key` HTTP parameters, as used within the `/action/wirelessConnect` handler.	8.8	More Details
CVE-2022-35885	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from format string injection via the `wpapsk_hex` HTTP parameter, as used within the `/action/wirelessConnect` handler.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35884	Four format string injection vulnerabilities exist in the web interface /action/wirelessConnect functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted HTTP request can lead to memory corruption, information disclosure and denial of service. An attacker can make an authenticated HTTP request to trigger these vulnerabilities.This vulnerability arises from format string injection via the `ssid_hex` HTTP parameter, as used within the `/action/wirelessConnect` handler.	8.8	More Details
CVE-2022-35881	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted UPnP negotiation can lead to memory corruption, information disclosure, and denial of service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `errorCode` and `errorDescription` XML tags, as used within the `DoUpdateUPnPbyService` action handler.	8.8	More Details
CVE-2022-35880	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted UPnP negotiation can lead to memory corruption, information disclosure, and denial of service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `NewInternalClient` XML tag, as used within the `DoUpdateUPnPbyService` action handler.	8.8	More Details
CVE-2022-35879	Four format string injection vulnerabilities exist in the UPnP logging functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9Z and 6.9X. A specially-crafted UPnP negotiation can lead to memory corruption, information disclosure, and denial of service. An attacker can host a malicious UPnP service to trigger these vulnerabilities.This vulnerability arises from format string injection via `controlURL` XML tag, as used within the `DoUpdateUPnPbyService` action handler.	8.8	More Details
CVE-2022-42198	In Simple Exam Reviewer Management System v1.0 the User List function suffers from insecure file upload.	8.8	More Details
CVE-2022-42199	Simple Exam Reviewer Management System v1.0 is vulnerable to Cross Site Request Forgery (CSRF) via the Exam List.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43407	Jenkins Pipeline: Input Step Plugin 451.vf1a_a_4f405289 and earlier does not restrict or sanitize the optionally specified ID of the 'input' step, which is used for the URLs that process user interactions for the given 'input' step (proceed or abort) and is not correctly encoded, allowing attackers able to configure Pipelines to have Jenkins build URLs from 'input' step IDs that would bypass the CSRF protection of any target URL in Jenkins when the 'input' step is interacted with.	8.8	More Details
CVE-2022-42344	Adobe Commerce versions 2.4.3-p2 (and earlier), 2.3.7-p3 (and earlier) and 2.4.4 (and earlier) are affected by an Incorrect Authorization vulnerability. An authenticated attacker can exploit this vulnerability to achieve information exposure and privilege escalation.	8.8	More Details
CVE-2022-36958	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with valid access to SolarWinds Web Console to execute arbitrary commands.	8.8	More Details
CVE-2022-43416	Jenkins Katalon Plugin 1.0.32 and earlier implements an agent/controller message that does not limit where it can be executed and allows invoking Katalon with configurable arguments, allowing attackers able to control agent processes to invoke Katalon on the Jenkins controller with attacker-controlled version, install location, and arguments, and attackers additionally able to create files on the Jenkins controller (e.g., attackers with Item/Configure permission could archive artifacts) to invoke arbitrary OS commands.	8.8	More Details
CVE-2022-35132	Usermin through 1.850 allows a remote authenticated user to execute OS commands via command injection in a filename for the GPG module.	8.8	More Details
CVE-2022-32775	An integer overflow vulnerability exists in the web interface /action/ipcamRecordPost functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to memory corruption. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2022-32586	An OS command injection vulnerability exists in the web interface /action/ipcamRecordPost functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30603	An OS command injection vulnerability exists in the web interface /action/iperf functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to arbitrary command execution. An attacker can make an authenticated HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2022-39267	Bifrost is a heterogeneous middleware that synchronizes MySQL, MariaDB to Redis, MongoDB, ClickHouse, MySQL and other services for production environments. Versions prior to 1.8.8-release are subject to authentication bypass in the admin and monitor user groups by deleting the X-Requested-With: XMLHttpRequest field in the request header. This issue has been patched in 1.8.8-release. There are no known workarounds.	8.8	More Details
CVE-2022-23734	A deserialization of untrusted data vulnerability was identified in GitHub Enterprise Server that could potentially lead to remote code execution on the SVNBridge. To exploit this vulnerability, an attacker would need to gain access via a server-side request forgery (SSRF) that would let an attacker control the data being deserialized. This vulnerability affected all versions of GitHub Enterprise Server prior to v3.6 and was fixed in versions 3.5.3, 3.4.6, 3.3.11, and 3.2.16. This vulnerability was reported via the GitHub Bug Bounty program.	8.8	More Details
CVE-2022-39326	kartverket/github-workflows are shared reusable workflows for GitHub Actions. Prior to version 2.7.5, all users of the `run-terraform` reusable workflow from the kartverket/github-workflows repo are affected by a code injection vulnerability. A malicious actor could potentially send a PR with a malicious payload leading to execution of arbitrary JavaScript code in the context of the workflow. Users should upgrade to at least version 2.7.5 to resolve the issue. As a workaround, review any pull requests from external users for malicious payloads before allowing them to trigger a build.	8.8	More Details
CVE-2022-36451	A vulnerability in the MiCollab Client server component of Mitel MiCollab through 9.5.0.101 could allow an authenticated attacker to conduct a Server-Side Request Forgery (SSRF) attack due to insufficient restriction of URL parameters. A successful exploit could allow an attacker to leverage connections and permissions available to the host server.	8.8	More Details
CVE-2022-1414	3scale API Management 2 does not perform adequate sanitation for user input in multiple fields. An authenticated user could use this flaw to inject scripts and possibly gain access to sensitive information or conduct further attacks.	8.8	More Details
CVE-2022-33183	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow a remote authenticated attacker to perform stack buffer overflow using in “firmwaredownload” and “diagshow” commands.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3395	The WP All Export Pro WordPress plugin before 1.7.9 uses the contents of the cc_sql POST parameter directly as a database query, allowing users which has been given permission to run exports to execute arbitrary SQL statements, leading to a SQL Injection vulnerability. By default only users with the Administrator role can perform exports, but this can be delegated to lower privileged users as well.	8.8	More Details
CVE-2022-3246	The Blog2Social: Social Media Auto Post & Scheduler WordPress plugin before 6.9.10 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by any authenticated users, such as subscribers	8.8	More Details
CVE-2022-33179	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, and 7.4.2j could allow a local authenticated user to break out of restricted shells with “set context” and escalate privileges.	8.8	More Details
CVE-2022-36453	A vulnerability in the MiCollab Client API of Mitel MiCollab 9.1.3 through 9.5.0.101 could allow an authenticated attacker to modify their profile parameters due to improper authorization controls. A successful exploit could allow the authenticated attacker to control another extension number.	8.8	More Details
CVE-2022-28169	Brocade Webtools in Brocade Fabric OS versions before Brocade Fabric OS versions v9.1.1, v9.0.1e, and v8.2.3c could allow a low privilege webtools, user, to gain elevated admin rights, or privileges, beyond what is intended or entitled for that user. By exploiting this vulnerability, a user whose role is not an admin can create a new user with an admin role using the operator session id. The issue was replicated after intercepting the admin, and operator authorization headers sent unencrypted and editing a user addition request to use the operator's authorization header.	8.8	More Details
CVE-2022-38181	The Arm Mali GPU kernel driver allows unprivileged users to access freed memory because GPU memory operations are mishandled. This affects Bifrost r0p0 through r38p1, and r39p0; Valhall r19p0 through r38p1, and r39p0; and Midgard r4p0 through r32p0.	8.8	More Details
CVE-2022-1738	Fuji Electric D300win prior to version 3.7.1.17 is vulnerable to an out-of-bounds read, which could allow an attacker to leak sensitive data from the process memory.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39260	Git is an open source, scalable, distributed revision control system. `git shell` is a restricted login shell that can be used to implement Git's push/pull functionality via SSH. In versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4, the function that splits the command arguments into an array improperly uses an `int` to represent the number of entries in the array, allowing a malicious actor to intentionally overflow the return value, leading to arbitrary heap writes. Because the resulting array is then passed to `execv()`, it is possible to leverage this attack to gain remote code execution on a victim machine. Note that a victim must first allow access to `git shell` as a login shell in order to be vulnerable to this attack. This problem is patched in versions 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 and users are advised to upgrade to the latest version. Disabling `git shell` access via remote logins is a viable short-term workaround.	8.5	More Details
CVE-2022-22077	Memory corruption in graphics due to use-after-free in graphics dispatcher logic in Snapdragon Mobile	8.4	More Details
CVE-2022-3608	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.2.0-alpha.	8.4	More Details
CVE-2022-25750	Memory corruption in BTHOST due to double free while music playback and calls over bluetooth headset in Snapdragon Mobile	8.4	More Details
CVE-2022-25723	Memory corruption in multimedia due to use after free during callback registration failure in Snapdragon Mobile	8.4	More Details
CVE-2022-33214	Memory corruption in display due to time-of-check time-of-use of metadata reserved size in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	8.4	More Details
CVE-2022-33210	Memory corruption in automotive multimedia due to use of out-of-range pointer offset while parsing command request packet with a very large type value. in Snapdragon Auto	8.4	More Details
CVE-2022-25661	Memory corruption due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1059	Aethon TUG Home Base Server versions prior to version 24 are affected by un unauthenticated attacker who can freely access hashed user credentials.	8.2	More Details
CVE-2022-1066	Aethon TUG Home Base Server versions prior to version 24 are affected by un unauthenticated attacker who can freely access hashed user credentials.	8.2	More Details
CVE-2022-27494	Aethon TUG Home Base Server versions prior to version 24 are affected by un unauthenticated attacker who can freely access hashed user credentials.	8.2	More Details
CVE-2022-1070	Aethon TUG Home Base Server versions prior to version 24 are affected by un unauthenticated attacker who can freely access hashed user credentials.	8.2	More Details
CVE-2022-26423	Aethon TUG Home Base Server versions prior to version 24 are affected by un unauthenticated attacker who can freely access hashed user credentials.	8.2	More Details
CVE-2022-25719	Information disclosure in WLAN due to improper length check while processing authentication handshake in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	8.2	More Details
CVE-2022-39301	sra-admin is a background rights management system that separates the front and back end. sra-admin version 1.1.1 has a storage cross-site scripting (XSS) vulnerability. After logging into the sra-admin background, an attacker can upload an html page containing xss attack code in "Personal Center" - "Profile Picture Upload" allowing theft of the user's personal information. This issue has been patched in 1.1.2. There are no known workarounds.	8.2	More Details
CVE-2022-29475	An information disclosure vulnerability exists in the XFINDER functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted man-in-the-middle attack can lead to increased privileges. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39327	Azure CLI is the command-line interface for Microsoft Azure. In versions previous to 2.40.0, Azure CLI contains a vulnerability for potential code injection. Critical scenarios are where a hosting machine runs an Azure CLI command where parameter values have been provided by an external source. The vulnerability is only applicable when the Azure CLI command is run on a Windows machine and with any version of PowerShell and when the parameter value contains the `&` or `|` symbols. If any of these prerequisites are not met, this vulnerability is not applicable. Users should upgrade to version 2.40.0 or greater to receive a a mitigation for the vulnerability.	8.1	More Details
CVE-2022-23241	Clustered Data ONTAP versions 9.11.1 through 9.11.1P2 with SnapLock configured FlexGroups are susceptible to a vulnerability which could allow an authenticated remote attacker to arbitrarily modify or delete WORM data prior to the end of the retention period.	8.1	More Details
CVE-2022-42933	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-42934	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-41709	Markdownify version 1.4.1 allows an external attacker to execute arbitrary code remotely on any client attempting to view a malicious markdown file through Markdownify. This is possible because the application has the "nodeIntegration" option enabled.	7.8	More Details
CVE-2022-41309	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-42935	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42937	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-42944	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-42938	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-42942	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-42941	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-42940	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-42939	A malicious crafted TGA file when consumed through DesignReview.exe application could lead to memory corruption vulnerability. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-41310	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42936	A malicious crafted .dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by write access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-42943	A malicious crafted dwf or .pct file when consumed through DesignReview.exe application could lead to memory corruption vulnerability by read access violation. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2022-33185	Several commands in Brocade Fabric OS before Brocade Fabric OS v.9.0.1e, and v9.1.0 use unsafe string functions to process user input. Authenticated local attackers could abuse these vulnerabilities to exploit stack-based buffer overflows, allowing arbitrary code execution as the root user account.	7.8	More Details
CVE-2022-41796	Untrusted search path vulnerability in the installer of Content Transfer (for Windows) Ver.1.3 and prior allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	7.8	More Details
CVE-2022-43040	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a heap buffer overflow via the function gf_isom_box_dump_start_ex at /isomedia/box_funcs.c.	7.8	More Details
CVE-2022-33184	A vulnerability in fab_seg.c.h libraries of all Brocade Fabric OS versions before Brocade Fabric OS v9.1.1, v9.0.1e, v8.2.3c, v8.2.0_cbn5, 7.4.2j could allow local authenticated attackers to exploit stack-based buffer overflows and execute arbitrary code as the root user account.	7.8	More Details
CVE-2022-33182	A privilege escalation vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, could allow a local authenticated user to escalate its privilege to root using switch commands “supportlink”, “firmwaredownload”, “portcfgupload, license, and “fosexec”.	7.8	More Details
CVE-2022-25660	Memory corruption due to double free issue in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	7.8	More Details
CVE-2022-33217	Memory corruption in Qualcomm IPC due to buffer copy without checking the size of input while starting communication with a compromised kernel. in Snapdragon Mobile	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38436	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-36122	The Automox Agent before 40 on Windows incorrectly sets permissions on key files.	7.8	More Details
CVE-2022-38435	Adobe Illustrator versions 26.4 (and earlier) and 25.4.7 (and earlier) are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2022-43042	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a heap buffer overflow via the function FixSDTPInTRAF at isomedia/isom_intern.c.	7.8	More Details
CVE-2020-12744	The MSI installer in Verint Desktop Resources 15.2 allows an unprivileged local user to elevate their privileges during install or repair.	7.8	More Details
CVE-2022-42176	In PCTechSoft PCSecure V5.0.8.xw, use of Hard-coded Credentials in configuration files leads to admin panel access.	7.8	More Details
CVE-2022-2069	The APDFL.dll in Siemens JT2Go prior to V13.3.0.5 and Siemens Teamcenter Visualization prior to V14.0.0.2 contains an out of bounds write past the fixed-length heap-based buffer while parsing specially crafted PDF files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2022-3577	An out-of-bounds memory write flaw was found in the Linux kernel’s Kid-friendly Wired Controller driver. This flaw allows a local user to crash or potentially escalate their privileges on the system. It is in bigben_probe of drivers/hid/hid-bigbenff.c. The reason is incorrect assumption - bigben devices all have inputs. However, malicious devices can break this assumption, leaking to out-of-bound write.	7.8	More Details
CVE-2022-3570	Multiple heap buffer overflows in tiffcrop.c utility in libtiff library Version 4.4.0 allows attacker to trigger unsafe or out of bounds memory access via crafted TIFF image file which could result into application crash, potential information disclosure or any other context-dependent impact	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41836	When an 'Attack Signature False Positive Mode' enabled security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate.	7.5	More Details
CVE-2022-41833	In all BIG-IP 13.1.x versions, when an iRule containing the HTTP::collect command is configured on a virtual server, undisclosed requests can cause Traffic Management Microkernel (TMM) to terminate.	7.5	More Details
CVE-2022-41832	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when a SIP profile is configured on a virtual server, undisclosed messages can cause an increase in memory resource utilization.	7.5	More Details
CVE-2022-37453	An issue was discovered in Softing OPC UA C++ SDK before 6.10. A buffer overflow or an excess allocation happens due to unchecked array and matrix bounds in structure data types.	7.5	More Details
CVE-2022-39823	An issue was discovered in Softing OPC UA C++ SDK 5.66 through 6.x before 6.10. An OPC/UA browse request exceeding the server limit on continuation points may cause a use-after-free error	7.5	More Details
CVE-2022-35263	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.This denial of service is in the `/action/import_file/` API.	7.5	More Details
CVE-2022-39313	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Versions prior to 4.10.17, and prior to 5.2.8 on the 5.x branch, crash when a file download request is received with an invalid byte range, resulting in a Denial of Service. This issue has been patched in versions 4.10.17, and 5.2.8. There are no known workarounds.	7.5	More Details
CVE-2022-35267	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.This denial of service is in the `/action/import_https_cert_file/` API.	7.5	More Details
CVE-2022-42890	A vulnerability in Batik of Apache XML Graphics allows an attacker to run Java code from untrusted SVG via JavaScript. This issue affects Apache XML Graphics prior to 1.16. Users are recommended to upgrade to version 1.16.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41704	A vulnerability in Batik of Apache XML Graphics allows an attacker to run untrusted Java code from an SVG. This issue affects Apache XML Graphics prior to 1.16. It is recommended to update to version 1.16.	7.5	More Details
CVE-2022-38870	Free5gc v3.2.1 is vulnerable to Information disclosure.	7.5	More Details
CVE-2022-35271	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.This denial of service is in the `/action/import_cert_file/` API.	7.5	More Details
CVE-2022-35270	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.This denial of service is in the `/action/import_wireguard_cert_file/` API.	7.5	More Details
CVE-2022-35269	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.This denial of service is in the `/action/import_e2c_json_file/` API.	7.5	More Details
CVE-2022-35268	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.This denial of service is in the `/action/import_sdk_file/` API.	7.5	More Details
CVE-2022-35266	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.This denial of service is in the `/action/import_firmware/` API.	7.5	More Details
CVE-2022-41986	Information disclosure vulnerability in Android App 'IIJ SmartKey' versions prior to 2.1.4 allows an attacker to obtain a one-time password issued by the product under certain conditions.	7.5	More Details
CVE-2022-35265	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.This denial of service is in the `/action/import_nodejs_app/` API.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35264	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.This denial of service is in the `/action/import_aaa_cert_file/` API.	7.5	More Details
CVE-2022-41787	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, when DNS profile is configured on a virtual server with DNS Express enabled, undisclosed DNS queries with DNSSEC can cause TMM to terminate.	7.5	More Details
CVE-2022-35262	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.This denial of service is in the `/action/import_xml_file/` API.	7.5	More Details
CVE-2022-35261	A denial of service vulnerability exists in the web_server hashFirst functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to denial of service. An attacker can send a sequence of requests to trigger this vulnerability.This denial of service is in the `/action/import_authorized_keys/` API.	7.5	More Details
CVE-2022-32760	A denial of service vulnerability exists in the XCMD doDebug functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted XCMD can lead to denial of service. An attacker can send a malicious XML payload to trigger this vulnerability.	7.5	More Details
CVE-2022-43680	In libexpat through 2.4.9, there is a use-after free caused by overeager destruction of a shared DTD in XML_ExternalEntityParserCreate in out-of-memory situations.	7.5	More Details
CVE-2022-41806	In versions 16.1.x before 16.1.3.2 and 15.1.x before 15.1.5.1, when BIG-IP AFM Network Address Translation policy with IPv6/IPv4 translation rules is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization.	7.5	More Details
CVE-2022-33077	An access control issue in nopcommerce v4.50.2 allows attackers to arbitrarily modify any customer's address via the addressedit endpoint.	7.5	More Details
CVE-2022-41575	A credential-exposure vulnerability in the support-bundle mechanism in Gradle Enterprise 2022.3 through 2022.3.3 allows remote attackers to access a subset of application data (e.g., cleartext credentials). This is fixed in 2022.3.3.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23648	Asus RT-N12E 2.0.0.39 is affected by an incorrect access control vulnerability. Through system.asp / start_apply.htm, an attacker can change the administrator password without any authentication.	7.5	More Details
CVE-2022-43429	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to read arbitrary files on the Jenkins controller file system.	7.5	More Details
CVE-2022-43430	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	7.5	More Details
CVE-2013-4253	The deployment script in the unsupported "OpenShift Extras" set of add-on scripts, in Red Hat Openshift 1, installs a default public key in the root user's authorized_keys file.	7.5	More Details
CVE-2022-43415	Jenkins REPO Plugin 1.15.0 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	7.5	More Details
CVE-2022-42227	jsonlint 1.0 is vulnerable to heap-buffer-overflow via /home/hjsz/jsonlint/src/lexer.	7.5	More Details
CVE-2022-25736	Denial of service in WLAN due to out-of-bound read happens while processing VHT action frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2022-25749	Transient Denial-of-Service in WLAN due to buffer over-read while parsing MDNS frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	7.5	More Details
CVE-2022-40798	OcoMon 4.0RC1 is vulnerable to Incorrect Access Control. Through a request the user can obtain the real email, sending the same request with correct email its possible to account takeover.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41624	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.2, 15.1.x before 15.1.7, 14.1.x before 14.1.5.2, and 13.1.x before 13.1.5.1, when a sideband iRule is configured on a virtual server, undisclosed traffic can cause an increase in memory resource utilization.	7.5	More Details
CVE-2022-41691	When a BIG-IP Advanced WAF/ASM security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate.	7.5	More Details
CVE-2022-27623	Missing authentication for critical function vulnerability in iSCSI management functionality in Synology DiskStation Manager (DSM) before 7.1-42661 allows remote attackers to read or write arbitrary files via unspecified vectors.	7.4	More Details
CVE-2022-41835	In F5OS-A version 1.x before 1.1.0 and F5OS-C version 1.x before 1.5.0, excessive file permissions in F5OS allows an authenticated local attacker to execute limited set of commands in a container and impact the F5OS controller.	7.3	More Details
CVE-2022-25687	memory corruption in video due to buffer overflow while parsing asf clips in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	7.3	More Details
CVE-2022-38104	Auth. WordPress Options Change (siteurl, users_can_register, default_role, admin_email and new_admin_email) vulnerability in Biplob Adhikari's Accordions – Multiple Accordions or FAQs Builder plugin (versions <= 2.0.3 on WordPress.	7.2	More Details
CVE-2022-3335	The Kadence WooCommerce Email Designer WordPress plugin before 1.5.7 unserialises the content of an imported file, which could lead to PHP object injections issues when an admin import (intentionally or not) a malicious file and a suitable gadget chain is present on the blog.	7.2	More Details
CVE-2022-3394	The WP All Export Pro WordPress plugin before 1.7.9 does not limit some functionality during exports only to users with the Administrator role, allowing any logged in user which has been given privileges to perform exports to execute arbitrary code on the site. By default only administrators can run exports, but the privilege can be delegated to lower privileged users.	7.2	More Details
CVE-2022-36957	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38108	SolarWinds Platform was susceptible to the Deserialization of Untrusted Data. This vulnerability allows a remote adversary with Orion admin-level account access to SolarWinds Web Console to execute arbitrary commands.	7.2	More Details
CVE-2022-42189	Emlog Pro 1.6.0 plugins upload suffers from a remote code execution (RCE) vulnerability.	7.2	More Details
CVE-2022-42201	Simple Exam Reviewer Management System v1.0 is vulnerable to Insecure file upload.	7.2	More Details
CVE-2022-41617	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5.1, and 13.1.x before 13.1.5.1, When the Advanced WAF / ASM module is provisioned, an authenticated remote code execution vulnerability exists in the BIG-IP iControl REST interface.	7.2	More Details
CVE-2022-3300	The Form Maker by 10Web WordPress plugin before 1.15.6 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2022-34850	An OS command injection vulnerability exists in the web_server /action/import_authorized_keys/ functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network request can lead to arbitrary command execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details
CVE-2022-31366	An arbitrary file upload vulnerability in the apiImportLabs function in api_labs.php of EVE-NG 2.0.3-112 Community allows attackers to execute arbitrary code via a crafted UNL file.	7.2	More Details
CVE-2021-46850	myVesta Control Panel before 0.9.8-26-43 and Vesta Control Panel before 0.9.8-26 are vulnerable to command injection. An authenticated and remote administrative user can execute arbitrary commands via the v_sftp_license parameter when sending HTTP POST requests to the /edit/server endpoint.	7.2	More Details
CVE-2022-33178	A vulnerability in the radius authentication system of Brocade Fabric OS before Brocade Fabric OS 9.0 could allow a remote attacker to execute arbitrary code on the Brocade switch.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3302	The Spam protection, AntiSpam, FireWall by CleanTalk WordPress plugin before 5.185.1 does not validate ids before using them in a SQL statement, which could lead to SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2022-41742	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted audio or video file. The issue affects only NGINX products that are built with the module ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module.	7.1	More Details
CVE-2022-41743	NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_hls_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its crash or potential other impact using a specially crafted audio or video file. The issue affects only NGINX Plus when the hls directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_hls_module.	7.0	More Details
CVE-2022-26870	Dell PowerStore versions 2.1.0.x contain an Authentication bypass vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability under specific configuration. An attacker would gain unauthorized access upon successful exploit.	7.0	More Details
CVE-2022-41741	NGINX Open Source before versions 1.23.2 and 1.22.1, NGINX Open Source Subscription before versions R2 P1 and R1 P1, and NGINX Plus before versions R27 P1 and R26 P1 have a vulnerability in the module ngx_http_mp4_module that might allow a local attacker to corrupt NGINX worker memory, resulting in its termination or potential other impact using a specially crafted audio or video file. The issue affects only NGINX products that are built with the ngx_http_mp4_module, when the mp4 directive is used in the configuration file. Further, the attack is possible only if an attacker can trigger processing of a specially crafted audio or video file with the module ngx_http_mp4_module.	7.0	More Details
CVE-2021-42553	A buffer overflow vulnerability in stm32_mw_usb_host of STMicroelectronics in versions before 3.5.1 allows an attacker to execute arbitrary code when the descriptor contains more endpoints than USBH_MAX_NUM_ENDPOINTS. The library is typically integrated when using a RTOS such as FreeRTOS on STM32 MCUs.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35860	Missing AES encryption in Corsair K63 Wireless 3.1.3 allows physically proximate attackers to inject and sniff keystrokes via 2.4 GHz radio transmissions.	6.8	More Details
CVE-2020-9285	Some versions of Sonos One (1st and 2nd generation) allow partial or full memory access via attacker controlled hardware that can be attached to the Mini-PCI Express slot on the motherboard that hosts the WiFi card on the device.	6.8	More Details
CVE-2022-25665	Information disclosure due to buffer over read in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile	6.8	More Details
CVE-2022-34438	Dell PowerScale OneFS, versions 8.2.x-9.4.0.x, contain a privilege context switching error. A local authenticated malicious user with high privileges could potentially exploit this vulnerability, leading to full system compromise. This impacts compliance mode clusters.	6.7	More Details
CVE-2022-34437	Dell PowerScale OneFS, versions 8.2.2-9.3.0, contain an OS command injection vulnerability. A privileged local malicious user could potentially exploit this vulnerability, leading to a full system compromise. This impacts compliance mode clusters.	6.7	More Details
CVE-2022-25666	Memory corruption due to use after free in service while trying to access maps by different threads in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	6.7	More Details
CVE-2022-31239	Dell PowerScale OneFS, versions 9.0.0 up to and including 9.1.0.19, 9.2.1.12, and 9.3.0.6, contain sensitive data in log files vulnerability. A privileged local user may potentially exploit this vulnerability, leading to disclosure of this sensitive data.	6.7	More Details
CVE-2022-43020	OpenCATS v0.9.6 was discovered to contain a SQL injection vulnerability via the tag_id variable in the Tag update function.	6.5	More Details
CVE-2022-41770	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, and BIG-IQ all versions of 8.x and 7.x, an authenticated iControl REST user can cause an increase in memory resource utilization, via undisclosed requests.	6.5	More Details
CVE-2022-43033	An issue was discovered in Bento4 1.6.0-639. There is a bad free in the component AP4_HdlrAtom::~AP4_HdlrAtom() which allows attackers to cause a Denial of Service (DoS) via a crafted input.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43034	An issue was discovered in Bento4 v1.6.0-639. There is a heap buffer overflow vulnerability in the AP4_BitReader::SkipBits(unsigned int) function in mp42ts.	6.5	More Details
CVE-2022-43035	An issue was discovered in Bento4 v1.6.0-639. There is a heap-buffer-overflow in AP4_Dec3Atom::AP4_Dec3Atom at Ap4Dec3Atom.cpp, leading to a Denial of Service (DoS), as demonstrated by mp42aac.	6.5	More Details
CVE-2022-43037	An issue was discovered in Bento4 1.6.0-639. There is a memory leak in the function AP4_File::ParseStream in /Core/Ap4File.cpp.	6.5	More Details
CVE-2022-43038	Bento4 v1.6.0-639 was discovered to contain a heap overflow via the AP4_BitReader::ReadCache() function in mp42ts.	6.5	More Details
CVE-2022-43408	Jenkins Pipeline: Stage View Plugin 2.26 and earlier does not correctly encode the ID of 'input' steps when using it to generate URLs to proceed or abort Pipeline builds, allowing attackers able to configure Pipelines to specify 'input' step IDs resulting in URLs that would bypass the CSRF protection of any target URL in Jenkins.	6.5	More Details
CVE-2022-42197	In Simple Exam Reviewer Management System v1.0 the User List function has improper access control that allows low privileged users to modify user permissions to higher privileges.	6.5	More Details
CVE-2022-33757	An authenticated attacker could read Nessus Debug Log file attachments from the web UI without having the correct privileges to do so. This may lead to the disclosure of information on the scan target and/or the Nessus scan to unauthorized parties able to reach the Nessus instance.	6.5	More Details
CVE-2022-32574	A double-free vulnerability exists in the web interface /action/ipcamSetParamPost functionality of Abode Systems, Inc. iota All-In-One Security Kit 6.9X and 6.9Z. A specially-crafted HTTP request can lead to memory corruption. An attacker can make an authenticated HTTP request to trigger this vulnerability.	6.5	More Details
CVE-2022-41707	Relatedcode's Messenger version 7bcd20b allows an authenticated external attacker to access sensitive data of any user of the application. This is possible because the application exposes user data to the public.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43419	Jenkins Katalon Plugin 1.0.32 and earlier stores API keys unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Extended Read permission, or access to the Jenkins controller file system.	6.5	More Details
CVE-2022-2805	A flaw was found in ovirt-engine, which leads to the logging of plaintext passwords in the log file when using otapi-style. This flaw allows an attacker with sufficient privileges to read the log file, leading to confidentiality loss.	6.5	More Details
CVE-2022-2762	The AdminPad WordPress plugin before 2.2 does not have CSRF check when updating admin's note, allowing attackers to make a logged in admin update their notes via a CSRF attack	6.5	More Details
CVE-2022-41799	Improper access control vulnerability in GROWI prior to v5.1.4 (v5 series) and versions prior to v4.5.25 (v4 series) allows a remote authenticated attacker to bypass access restriction and download the markdown data from the pages set to private by the other users.	6.5	More Details
CVE-2022-41797	Improper authorization in handler for custom URL scheme vulnerability in Lemon8 App for Android versions prior to 3.3.5 and Lemon8 App for iOS versions prior to 3.3.5 allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App. As a result, the user may become a victim of a phishing attack.	6.5	More Details
CVE-2022-3676	In Eclipse Openj9 before version 0.35.0, interface calls can be inlined without a runtime type check. Malicious bytecode could make use of this inlining to access or modify memory via an incompatible type.	6.5	More Details
CVE-2022-41813	In versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, when BIG-IP is provisioned with PEM or AFM module, an undisclosed input can cause Traffic Management Microkernel (TMM) to terminate.	6.5	More Details
CVE-2022-28170	Brocade Fabric OS Web Application services before Brocade Fabric v9.1.0, v9.0.1e, v8.2.3c, v7.4.2j store server and user passwords in the debug statements. This could allow a local user to extract the passwords from a debug file.	6.5	More Details
CVE-2021-44776	A broken access control vulnerability in the SubNet_handler_func function of spx_restservice allows an attacker to arbitrarily change the security access rights to KVM and Virtual Media functionalities. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36783	AlgoSec – FireFlow Reflected Cross-Site-Scripting (RXSS) A malicious user injects JavaScript code into a parameter called IntersectudRule on the search/result.html page. The malicious user changes the request from POST to GET and sends the URL to another user (victim). JavaScript code is executed on the browser of the other user.	6.5	More Details
CVE-2022-43032	An issue was discovered in Bento4 v1.6.0-639. There is a memory leak in AP4_DescriptorFactory::CreateDescriptorFromStream in Core/Ap4DescriptorFactory.cpp, as demonstrated by mp42aac.	6.5	More Details
CVE-2022-36454	A vulnerability in the MiCollab Client API of Mitel MiCollab through 9.5.0.101 could allow an authenticated attacker to modify their profile parameters due to improper authorization controls. A successful exploit could allow the authenticated attacker to impersonate another user's name.	6.5	More Details
CVE-2022-39315	Kirby is a Content Management System. Prior to versions 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1, a user enumeration vulnerability affects all Kirby sites with user accounts unless Kirby's API and Panel are disabled in the config. It can only be exploited for targeted attacks because the attack does not scale to brute force. The problem has been patched in Kirby 3.5.8.2, Kirby 3.6.6.2, Kirby 3.7.5.1, and Kirby 3.8.1. In all of the mentioned releases, the maintainers have rewritten the affected code so that the delay is also inserted after the brute force limit is reached.	6.5	More Details
CVE-2022-3247	The Blog2Social: Social Media Auto Post & Scheduler WordPress plugin before 6.9.10 does not have authorisation in an AJAX action, and does not ensure that the URL to make a request to is an external one. As a result, any authenticated users, such as subscriber could perform SSRF attacks	6.5	More Details
CVE-2022-43021	OpenCATS v0.9.6 was discovered to contain a SQL injection vulnerability via the entriesPerPage variable.	6.5	More Details
CVE-2022-3097	The Plugin LBstopattack WordPress plugin before 1.1.3 does not use nonces when saving its settings, making it possible for attackers to conduct CSRF attacks. This could allow attackers to disable the plugin's protections.	6.5	More Details
CVE-2022-43022	OpenCATS v0.9.6 was discovered to contain a SQL injection vulnerability via the tag_id variable in the Tag deletion function.	6.5	More Details
CVE-2022-43023	OpenCATS v0.9.6 was discovered to contain a SQL injection vulnerability via the importID parameter in the Import viewerrors function.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26732	A broken access control vulnerability in the First_network_func function of spx_restservice allows an attacker to arbitrarily change the network configuration of the BMC. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	6.5	More Details
CVE-2022-38196	Esri ArcGIS Server versions 10.9.1 and prior have a path traversal vulnerability that may result in a denial of service by allowing a remote, authenticated attacker to overwrite internal ArcGIS Server directory.	6.5	More Details
CVE-2022-23462	IOWOW is a C utility library and persistent key/value storage engine. Versions 1.4.15 and prior contain a stack buffer overflow vulnerability that allows for Denial of Service (DOS) when it parses scientific notation numbers present in JSON. A patch for this issue is available at commit a79d31e4cff1d5a08f665574b29fd885897a28fd in the `master` branch of the repository. There are no workarounds other than applying the patch.	6.2	More Details
CVE-2022-25664	Information disclosure due to exposure of information while GPU reads the data in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	6.2	More Details
CVE-2022-43014	OpenCATS v0.9.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the joborderID parameter.	6.1	More Details
CVE-2022-38195	There is as reflected cross site scripting issue in Esri ArcGIS Server versions 10.9.1 and below which may allow a remote unauthorized attacker able to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the victim’s browser.	6.1	More Details
CVE-2022-43017	OpenCATS v0.9.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the indexFile component.	6.1	More Details
CVE-2022-43016	OpenCATS v0.9.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the callback component.	6.1	More Details
CVE-2022-38197	Esri ArcGIS Server versions 10.9.1 and below have an unvalidated redirect issue that may allow a remote, unauthenticated attacker to phish a user into accessing an attacker controlled website via a crafted query parameter.	6.1	More Details
CVE-2022-1523	Fuji Electric D300win prior to version 3.7.1.17 is vulnerable to a write-what-where condition, which could allow an attacker to overwrite program memory to manipulate the flow of information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31468	OX App Suite through 8.2 allows XSS via an attachment or OX Drive content when a client uses the len or off parameter.	6.1	More Details
CVE-2022-27913	An issue was discovered in Joomla! 4.2.0 through 4.2.3. Inadequate filtering of potentially malicious user input leads to reflected XSS vulnerabilities in various components.	6.1	More Details
CVE-2022-26954	Multiple open redirect vulnerabilities in NopCommerce 4.10 through 4.50.1 allow remote attackers to conduct phishing attacks by redirecting users to attacker-controlled web sites via the returnUrl parameter, processed by the (1) ChangePassword function, (2) SignInCustomerAsync function, (3) SuccessfulAuthentication method, or (4) NopRedirectResultExecutor class.	6.1	More Details
CVE-2022-43018	OpenCATS v0.9.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the email parameter in the Check Email function.	6.1	More Details
CVE-2022-38198	There is a reflected cross site scripting issue in the Esri ArcGIS Server services directory versions 10.9.1 and below that may allow a remote, unauthenticated attacker to convince a user to click on a crafted link which could potentially execute arbitrary JavaScript code in the victim’s browser.	6.1	More Details
CVE-2022-43015	OpenCATS v0.9.6 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the entriesPerPage parameter.	6.1	More Details
CVE-2022-42466	Prior to 2.0.0-M9, it was possible for an end-user to set the value of an editable string property of a domain object to a value that would be rendered unchanged when the value was saved. In particular, the end-user could enter javascript or similar and this would be executed. As of this release, the inputted strings are properly escaped when rendered.	6.1	More Details
CVE-2022-38200	A cross site scripting vulnerability exists in some map service configurations of ArcGIS Server versions 10.8.1 and 10.7.1. Specifically crafted web requests can execute arbitrary JavaScript in the context of the victim's browser.	6.1	More Details
CVE-2022-38199	A remote file download issue can occur in some capabilities of Esri ArcGIS Server web services that may in some edge cases allow a remote, unauthenticated attacker to induce an unsuspecting victim to launch a process in the victim's PATH environment. Current browsers provide users with warnings against running unsigned executables downloaded from the internet.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38162	Reflected cross-site scripting (XSS) vulnerabilities in WithSecure through 2022-08-10) exists within the F-Secure Policy Manager due to an unvalidated parameter in the endpoint, which allows remote attackers to provide a malicious input.	6.1	More Details
CVE-2022-3607	Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) in GitHub repository octoprint/octoprint prior to 1.8.3.	6.0	More Details
CVE-2022-39341	OpenFGA is an authorization/permission engine. Versions prior to version 0.2.4 are vulnerable to authorization bypass under certain conditions. Users who have wildcard (`*`) defined on tupleset relations in their authorization model are vulnerable. Version 0.2.4 contains a patch for this issue.	5.9	More Details
CVE-2022-39342	OpenFGA is an authorization/permission engine. Versions prior to version 0.2.4 are vulnerable to authorization bypass under certain conditions. Users whose model has a relation defined as a tupleset (the right hand side of a ‘from’ statement) that involves anything other than a direct relationship (e.g. ‘as self’) are vulnerable. Version 0.2.4 contains a patch for this issue.	5.9	More Details
CVE-2022-39354	SputnikVM, also called evm, is a Rust implementation of Ethereum Virtual Machine. A custom stateful precompile can use the `is_static` parameter to determine if the call is executed in a static context (via `STATICCALL`), and thus decide if stateful operations should be done. Prior to version 0.36.0, the passed `is_static` parameter was incorrect -- it was only set to `true` if the call came from a direct `STATICCALL` opcode. However, once a static call context is entered, it should stay static. The issue only impacts custom precompiles that actually uses `is_static`. For those affected, the issue can lead to possible incorrect state transitions. Version 0.36.0 contains a patch. There are no known workarounds.	5.9	More Details
CVE-2021-4228	Use of hard-coded TLS certificate by default allows an attacker to perform Man-in-the-Middle (MitM) attacks even in the presence of the HTTPS connection. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.00.0.	5.8	More Details
CVE-2021-46279	Session fixation and insufficient session expiration vulnerabilities allow an attacker to perfom session hijacking attacks against users. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3620	A vulnerability was found in Exim and classified as problematic. This issue affects the function dmarc_dns_lookup of the file dmarc.c of the component DMARC Handler. The manipulation leads to use after free. The attack may be initiated remotely. The name of the patch is 12fb3842f81bcbd4a4519d5728f2d7e0e3ca1445. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211919.	5.6	More Details
CVE-2022-3598	LibTIFF 4.4.0 has an out-of-bounds write in extractContigSamplesShifted24bits in tools/tiffcrop.c:3604, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit cfbb883b.	5.5	More Details
CVE-2022-3626	LibTIFF 4.4.0 has an out-of-bounds write in _TIFFmemset in libtiff/tif_unix.c:340 when called from processCropSelections, tools/tiffcrop.c:7619, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 236b7191.	5.5	More Details
CVE-2013-4281	In Red Hat Openshift 1, weak default permissions are applied to the /etc/openshift/server_priv.pem file on the broker server, which could allow users with local access to the broker to read this file.	5.5	More Details
CVE-2022-3344	A flaw was found in the KVM's AMD nested virtualization (SVM). A malicious L1 guest could purposely fail to intercept the shutdown of a cooperative nested guest (L2), possibly leading to a page fault and kernel panic in the host (L0).	5.5	More Details
CVE-2022-43045	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a segmentation violation via the function gf_dump_vrml_sffield at /scene_manager/scene_dump.c.	5.5	More Details
CVE-2022-43044	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a segmentation violation via the function gf_isom_get_meta_item_info at /isomedia/meta.c.	5.5	More Details
CVE-2022-43043	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a segmentation violation via the function BD_CheckSFTimeOffset at /bifs/field_decode.c.	5.5	More Details
CVE-2022-43039	GPAC 2.1-DEV-rev368-gfd054169b-master was discovered to contain a segmentation violation via the function gf_isom_meta_restore_items_ref at /isomedia/meta.c.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39837	An issue was discovered in Connected Vehicle Systems Alliance (COVESA) dlt-daemon through 2.18.8. Due to a faulty DLT file parser, a crafted DLT file that crashes the process can be created. This is due to missing validation checks. There is a NULL pointer dereference,	5.5	More Details
CVE-2022-3627	LibTIFF 4.4.0 has an out-of-bounds write in _TIFFmemcpy in libtiff/tif_unix.c:346 when called from extractImageSection, tools/tiffcrop.c:6860, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 236b7191.	5.5	More Details
CVE-2022-3599	LibTIFF 4.4.0 has an out-of-bounds read in writeSingleSection in tools/tiffcrop.c:7345, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit e8131125.	5.5	More Details
CVE-2022-3644	The collection remote for pulp_ansible stores tokens in plaintext instead of using pulp's encrypted field and exposes them in read/write mode via the API () instead of marking it as write only.	5.5	More Details
CVE-2022-3597	LibTIFF 4.4.0 has an out-of-bounds write in _TIFFmemcpy in libtiff/tif_unix.c:346 when called from extractImageSection, tools/tiffcrop.c:6826, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 236b7191.	5.5	More Details
CVE-2022-3586	A flaw was found in the Linux kernel’s networking code. A use-after-free was found in the way the sch_sfb enqueue function used the socket buffer (SKB) cb field after the same SKB had been enqueued (and freed) into a child qdisc. This flaw allows a local, unprivileged user to crash the system, causing a denial of service.	5.5	More Details
CVE-2022-40884	Bento4 1.6.0 has memory leaks via the mp4fragment.	5.5	More Details
CVE-2022-40885	Bento4 v1.6.0-639 has a memory allocation issue that can cause denial of service.	5.5	More Details
CVE-2022-3640	A vulnerability, which was classified as critical, was found in Linux Kernel. Affected is the function l2cap_conn_del of the file net/bluetooth/l2cap_core.c of the component Bluetooth. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211944.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39836	An issue was discovered in Connected Vehicle Systems Alliance (COVESA) dlt-daemon through 2.18.8. Due to a faulty DLT file parser, a crafted DLT file that crashes the process can be created. This is due to missing validation checks. There is a heap-based buffer over-read of one byte.	5.5	More Details
CVE-2022-39253	Git is an open source, scalable, distributed revision control system. Versions prior to 2.30.6, 2.31.5, 2.32.4, 2.33.5, 2.34.5, 2.35.5, 2.36.3, and 2.37.4 are subject to exposure of sensitive information to a malicious actor. When performing a local clone (where the source and target of the clone are on the same volume), Git copies the contents of the source's `$GIT_DIR/objects` directory into the destination by either creating hardlinks to the source contents, or copying them (if hardlinks are disabled via `--no-hardlinks`). A malicious actor could convince a victim to clone a repository with a symbolic link pointing at sensitive information on the victim's machine. This can be done either by having the victim clone a malicious repository on the same machine, or having them clone a malicious repository embedded as a bare repository via a submodule from any source, provided they clone with the `--recurse-submodules` option. Git does not create symbolic links in the `$GIT_DIR/objects` directory. The problem has been patched in the versions published on 2022-10-18, and backported to v2.30.x. Potential workarounds: Avoid cloning untrusted repositories using the `--local` optimization when on a shared machine, either by passing the `--no-local` option to `git clone` or cloning from a URL that uses the `file://` scheme. Alternatively, avoid cloning repositories from untrusted sources with `--recurse-submodules` or run `git config --global protocol.file.allow user`.	5.5	More Details
CVE-2022-39349	The Tasks.org Android app is an open-source app for to-do lists and reminders. The Tasks.org app uses the activity `ShareLinkActivity.kt` to handle "share" intents coming from other components in the same device and convert them to tasks. Those intents may contain arbitrary file paths as attachments, in which case the files pointed by those paths are copied in the app's external storage directory. Prior to versions 12.7.1 and 13.0.1, those paths were not validated, allowing a malicious or compromised application in the same device to force Tasks.org to copy files from its internal storage to its external storage directory, where they became accessible to any component with permission to read the external storage. This vulnerability can lead to sensitive information disclosure. All information in the user's notes and the app's preferences, including the encrypted credentials of CalDav integrations if enabled, could be accessed by third party applications installed on the same device. This issue was fixed in versions 12.7.1 and 13.0.1. There are no known workarounds.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3636	A vulnerability, which was classified as critical, was found in Linux Kernel. This affects the function __mtk_ppe_check_skb of the file drivers/net/ethernet/mediatek/mtk_ppe.c of the component Ethernet Handler. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211935.	5.5	More Details
CVE-2022-25663	Possible buffer overflow due to lack of buffer length check during management frame Rx handling lead to denial of service in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity	5.5	More Details
CVE-2022-3635	A vulnerability, which was classified as critical, has been found in Linux Kernel. Affected by this issue is the function tst_timer of the file drivers/atm/idt77252.c of the component IPsec. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. VDB-211934 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2022-41780	In F5OS-A version 1.x before 1.1.0 and F5OS-C version 1.x before 1.4.0, a directory traversal vulnerability exists in an undisclosed location of the F5OS CLI that allows an attacker to read arbitrary files.	5.5	More Details
CVE-2022-33181	An information disclosure vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5, 7.4.2.j could allow a local authenticated attacker to read sensitive files using switch commands “configshow” and “supportlink”.	5.5	More Details
CVE-2022-43677	In free5GC 3.2.1, a malformed NGAP message can crash the AMF and NGAP decoders via an index-out-of-range panic in aper.GetBitString.	5.5	More Details
CVE-2022-33180	A vulnerability in Brocade Fabric OS CLI before Brocade Fabric OS v9.1.0, 9.0.1e, 8.2.3c, 8.2.0cbn5 could allow a local authenticated attacker to export out sensitive files with “seccryptocfg”, “configupload”.	5.5	More Details
CVE-2022-38117	Juiker app hard-coded its AES key in the source code. A physical attacker, after getting the Android root privilege, can use the AES key to decrypt users’ ciphertext and tamper with it.	5.5	More Details
CVE-2022-43425	Jenkins Custom Checkbox Parameter Plugin 1.4 and earlier does not escape the name and description of Custom Checkbox Parameter parameters on views displaying parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43409	Jenkins Pipeline: Supporting APIs Plugin 838.va_3a_087b_4055b and earlier does not sanitize or properly encode URLs of hyperlinks sending POST requests in build logs, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to create Pipelines.	5.4	More Details
CVE-2022-38901	A Cross-site scripting (XSS) vulnerability in the Document and Media module - file upload functionality in Liferay Digital Experience Platform 7.3.10 SP3 allows remote attackers to inject arbitrary JS script or HTML into the description field of uploaded svg file.	5.4	More Details
CVE-2022-39350	@dependencytrack/frontend is a Single Page Application (SPA) used in Dependency-Track, an open source Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain. Due to the common practice of providing vulnerability details in markdown format, the Dependency-Track frontend renders them using the JavaScript library Showdown. Showdown does not have any XSS countermeasures built in, and versions before 4.6.1 of the Dependency-Track frontend did not encode or sanitize Showdown's output. This made it possible for arbitrary JavaScript included in vulnerability details via HTML attributes to be executed in context of the frontend. Actors with the `VULNERABILITY_MANAGEMENT` permission can exploit this weakness by creating or editing a custom vulnerability and providing XSS payloads in any of the following fields: Description, Details, Recommendation, or References. The payload will be executed for users with the `VIEW_PORTFOLIO` permission when browsing to the modified vulnerability's page. Alternatively, malicious JavaScript could be introduced via any of the vulnerability databases mirrored by Dependency-Track. However, this attack vector is highly unlikely, and the maintainers of Dependency-Track are not aware of any occurrence of this happening. Note that the `Vulnerability Details` element of the `Audit Vulnerabilities` tab in the project view is not affected. The issue has been fixed in frontend version 4.6.1.	5.4	More Details
CVE-2022-42205	PHPGurukul Hospital Management System In PHP V 4.0 is vulnerable to Cross Site Scripting (XSS) via add-patient.php.	5.4	More Details
CVE-2022-42206	PHPGurukul Hospital Management System In PHP V 4.0 is vulnerable to Cross Site Scripting (XSS) via doctor/view-patient.php, admin/view-patient.php, and view-medhistory.php.	5.4	More Details
CVE-2022-36966	Users with Node Management rights were able to view and edit all nodes due to Insufficient control on URL parameter causing insecure direct object reference (IDOR) vulnerability in SolarWinds Platform 2022.3 and previous.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41358	A stored cross-site scripting (XSS) vulnerability in Garage Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the categoriesName parameter in createCategories.php.	5.4	More Details
CVE-2022-40690	Cross-site scripting vulnerability in BookStack versions prior to v22.09 allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2022-43185	A stored cross-site scripting (XSS) vulnerability in the Configuration/Holidays module of Rukovoditel v3.2.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter.	5.4	More Details
CVE-2022-41638	Auth. Stored Cross-Site Scripting (XSS) in Pop-Up Chop Chop plugin <= 2.1.7 on WordPress.	5.4	More Details
CVE-2021-33231	Cross Site Scripting (XSS) vulnerability in New equipment page in EasyVista Service Manager 2018.1.181.1 allows remote attackers to run arbitrary code via the notes field.	5.4	More Details
CVE-2022-43420	Jenkins Contrast Continuous Application Security Plugin 3.9 and earlier does not escape data returned from the Contrast service when generating a report, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control or modify Contrast service API responses.	5.4	More Details
CVE-2022-34870	Apache Geode versions up to 1.15.0 are vulnerable to a Cross-Site Scripting (XSS) via data injection when using Pulse web application to view Region entries.	5.4	More Details
CVE-2022-42200	Simple Exam Reviewer Management System v1.0 is vulnerable to Stored Cross Site Scripting (XSS) via the Exam List.	5.4	More Details
CVE-2022-43428	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process.	5.3	More Details
CVE-2022-34439	Dell PowerScale OneFS, versions 8.2.0.x-9.4.0.x contain allocation of Resources Without Limits or Throttling vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service and performance issue on that node.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43422	Jenkins Compuware Topaz Utilities Plugin 1.0.8 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process.	5.3	More Details
CVE-2021-26733	A broken access control vulnerability in the FirstReset_handler_func function of spx_restservice allows an attacker to arbitrarily send reboot commands to the BMC, causing a Denial-of-Service (DoS) condition. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	5.3	More Details
CVE-2022-25662	Information disclosure due to untrusted pointer dereference in kernel in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	5.3	More Details
CVE-2021-44467	A broken access control vulnerability in the KillDupUsr_func function of spx_restservice allows an attacker to arbitrarily terminate active sessions of other users, causing a Denial-of-Service (DoS) condition, if an input parameter is correctly guessed. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	5.3	More Details
CVE-2022-43421	A missing permission check in Jenkins Tuleap Git Branch Source Plugin 3.2.4 and earlier allows unauthenticated attackers to trigger Tuleap projects whose configured repository matches the attacker-specified value.	5.3	More Details
CVE-2022-43434	Jenkins NeuVector Vulnerability Scanner Plugin 1.20 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download.	5.3	More Details
CVE-2022-38107	Sensitive information could be displayed when a detailed technical error message is posted. This information could disclose environmental details.	5.3	More Details
CVE-2021-45925	Observable discrepancies in the login process allow an attacker to guess legitimate user names registered in the BMC. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	5.3	More Details
CVE-2022-43435	Jenkins 360 FireLine Plugin 1.7.2 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download.	5.3	More Details
CVE-2022-43424	Jenkins Compuware Xpediter Code Coverage Plugin 1.0.7 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36795	In BIG-IP versions 17.0.x before 17.0.0.1, 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, and 14.1.x before 14.1.5.1, when an LTM TCP profile with Auto Receive Window Enabled is configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections.	5.3	More Details
CVE-2022-42467	When running in prototype mode, the h2 webconsole module (accessible from the Prototype menu) is automatically made available with the ability to directly query the database. It was felt that it is safer to require the developer to explicitly enable this capability. As of 2.0.0-M8, this can now be done using the 'isis.prototyping.h2-console.web-allow-remote-access' configuration property; the web console will be unavailable without setting this configuration. As an additional safeguard, the new 'isis.prototyping.h2-console.generate-random-web-admin-password' configuration parameter (enabled by default) requires that the administrator use a randomly generated password to use the console. The password is printed to the log, as "webAdminPass: xxx" (where "xxx") is the password. To revert to the original behaviour, the administrator would therefore need to set these configuration parameter: isis.prototyping.h2-console.web-allow-remote-access=true isis.prototyping.h2-console.generate-random-web-admin-password=false Note also that the h2 webconsole is never available in production mode, so these safeguards are only to ensure that the webconsole is secured by default also in prototype mode.	5.3	More Details
CVE-2022-43412	Jenkins Generic Webhook Trigger Plugin 1.84.1 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	5.3	More Details
CVE-2022-43426	Jenkins S3 Explorer Plugin 1.0.8 and earlier does not mask the AWS_SECRET_ACCESS_KEY form field, increasing the potential for attackers to observe and capture it.	5.3	More Details
CVE-2022-39340	OpenFGA is an authorization/permission engine. Prior to version 0.2.4, the `streamed-list-objects` endpoint was not validating the authorization header, resulting in disclosure of objects in the store. Users `openfga/openfga` versions 0.2.3 and prior who are exposing the OpenFGA service to the internet are vulnerable. Version 0.2.4 contains a patch for this issue.	5.3	More Details
CVE-2022-3576	A vulnerability regarding out-of-bounds read is found in the session processing functionality of Out-of-Band (OOB) Management. This allows remote attackers to obtain sensitive information via unspecified vectors. The following models with Synology DiskStation Manager (DSM) versions before 7.1.1-42962-2 may be affected: DS3622xs+, FS3410, and HD6500.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35739	PRTG Network Monitor through 22.2.77.2204 does not prevent custom input for a device's icon, which can be modified to insert arbitrary content into the style tag for that device. When the device page loads, the arbitrary Cascading Style Sheets (CSS) data is inserted into the style tag, loading malicious content. Due to PRTG Network Monitor preventing "characters, and from modern browsers disabling JavaScript support in style tags, this vulnerability could not be escalated into a Cross-Site Scripting vulnerability.	5.3	More Details
CVE-2022-40084	OpenCRX before v5.2.2 was discovered to be vulnerable to password enumeration due to the difference in error messages received during a password reset which could enable an attacker to determine if a username, email or ID is valid.	5.3	More Details
CVE-2022-43423	Jenkins Compuware Source Code Download for Endevor, PDS, and ISPW Plugin 2.0.12 and earlier implements an agent/controller message that does not limit where it can be executed, allowing attackers able to control agent processes to obtain the values of Java system properties from the Jenkins controller process.	5.3	More Details
CVE-2022-43414	Jenkins NUnit Plugin 0.27 and earlier implements an agent-to-controller message that parses files inside a user-specified directory as test results, allowing attackers able to control agent processes to obtain test results from files in an attacker-specified directory on the Jenkins controller.	5.3	More Details
CVE-2022-43410	Jenkins Mercurial Plugin 1251.va_b_121f184902 and earlier provides information about which jobs were triggered or scheduled for polling through its webhook endpoint, including jobs the user has no permission to access.	5.3	More Details
CVE-2022-43411	Jenkins GitLab Plugin 1.5.35 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	5.3	More Details
CVE-2022-27912	An issue was discovered in Joomla! 4.0.0 through 4.2.3. Sites with publicly enabled debug mode exposed data of previous requests.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39272	Flux is an open and extensible continuous delivery solution for Kubernetes. Versions prior to 0.35.0 are subject to a Denial of Service. Users that have permissions to change Flux's objects, either through a Flux source or directly within a cluster, can provide invalid data to fields `.spec.interval` or `.spec.timeout` (and structured variations of these fields), causing the entire object type to stop being processed. This issue is patched in version 0.35.0. As a workaround, Admission controllers can be employed to restrict the values that can be used for fields `.spec.interval` and `.spec.timeout`, however upgrading to the latest versions is still the recommended mitigation.	5.0	More Details
CVE-2022-3623	A vulnerability was found in Linux Kernel. It has been declared as problematic. Affected by this vulnerability is the function follow_page_pte of the file mm/gup.c of the component BPF. The manipulation leads to race condition. The attack can be launched remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211921 was assigned to this vulnerability.	5.0	More Details
CVE-2022-41694	In BIG-IP versions 16.1.x before 16.1.3, 15.1.x before 15.1.6.1, 14.1.x before 14.1.5, and all versions of 13.1.x, and BIG-IQ versions 8.x before 8.2.0.1 and all versions of 7.x, when an SSL key is imported on a BIG-IP or BIG-IQ system, undisclosed input can cause MCPD to terminate.	4.9	More Details
CVE-2021-44769	An improper input validation vulnerability in the TLS certificate generation function allows an attacker to cause a Denial-of-Service (DoS) condition which can only be reverted via a factory reset. This issue affects: Lanner Inc IAC-AST2500A standard firmware version 1.10.0.	4.9	More Details
CVE-2022-3391	The Retain Live Chat WordPress plugin through 0.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-36368	Multiple stored cross-site scripting vulnerabilities in the web user interface of IPFire versions prior to 2.27 allows a remote authenticated attacker with administrative privilege to inject an arbitrary script.	4.8	More Details
CVE-2022-40311	Auth. (admin+) Stored Cross-Site Scripting (XSS) in Fatcat Apps Analytics Cat plugin <= 1.0.9 on WordPress.	4.8	More Details
CVE-2022-3392	The WP Humans.txt WordPress plugin through 1.0.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3350	The Contact Bank WordPress plugin through 3.0.30 does not sanitise and escape some of its Form settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-22078	Denial of service in BOOT when partition size for a particular partition is requested due to integer overflow when blocks are calculated in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	4.6	More Details
CVE-2022-3625	A vulnerability was found in Linux Kernel. It has been classified as critical. This affects the function devlink_param_set/devlink_param_get of the file net/core/devlink.c of the component IPsec. The manipulation leads to use after free. It is recommended to apply a patch to fix this issue. The identifier VDB-211929 was assigned to this vulnerability.	4.6	More Details
CVE-2022-39351	Dependency-Track is a Component Analysis platform that allows organizations to identify and reduce risk in the software supply chain. Prior to version 4.6.0, performing an API request using a valid API key with insufficient permissions causes the API key to be written to Dependency-Track's audit log in clear text. Actors with access to the audit log can exploit this flaw to gain access to valid API keys. The issue has been fixed in Dependency-Track 4.6.0. Instead of logging the entire API key, only the last 4 characters of the key will be logged. It is strongly recommended to check historic logs for occurrences of this behavior, and re-generating API keys in case of leakage.	4.4	More Details
CVE-2022-43418	A cross-site request forgery (CSRF) vulnerability in Jenkins Katalon Plugin 1.0.33 and earlier allows attackers to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	4.3	More Details
CVE-2022-41708	Relatedcode's Messenger version 7bcd20b allows an authenticated external attacker to access existing chats in the workspaces of any user of the application. This is possible because the application does not validate permissions correctly.	4.3	More Details
CVE-2022-43433	Jenkins ScreenRecorder Plugin 0.7 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download.	4.3	More Details
CVE-2022-43431	Jenkins Compuware Strobe Measurement Plugin 1.0.1 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31684	Reactor Netty HTTP Server, in versions 1.0.11 - 1.0.23, may log request headers in some cases of invalid HTTP requests. The logged headers may reveal valid access tokens to those with access to server logs. This may affect only invalid HTTP requests where logging at WARN level is enabled.	4.3	More Details
CVE-2022-43417	Jenkins Katalon Plugin 1.0.32 and earlier does not perform permission checks in several HTTP endpoints, allowing attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	4.3	More Details
CVE-2022-43427	Jenkins Compuware Topaz for Total Test Plugin 2.4.8 and earlier does not perform permission checks in several HTTP endpoints, allowing attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2022-43413	Jenkins Job Import Plugin 3.5 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	4.3	More Details
CVE-2022-3621	A vulnerability was found in Linux Kernel. It has been classified as problematic. Affected is the function nilfs_bmap_lookup_at_level of the file fs/nilfs2/inode.c of the component nilfs2. The manipulation leads to null pointer dereference. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211920.	4.3	More Details
CVE-2022-3639	A potential DOS vulnerability was discovered in GitLab CE/EE affecting all versions from 10.8 before 15.1.6, all versions starting from 15.2 before 15.2.4, all versions starting from 15.3 before 15.3.2. Improper data handling on branch creation could have been used to trigger high CPU usage.	4.3	More Details
CVE-2022-39233	Tuleap is a Free & Open Source Suite to improve management of software developments and collaboration. In versions 12.9.99.228 and above, prior to 14.0.99.24, authorizations are not properly verified when updating the branch prefix used by the GitLab repository integration. Authenticated users can change the branch prefix of any of the GitLab repository integration they can see vie the REST endpoint `PATCH /gitlab_repositories/{id}`. This action should be restricted to Git administrators. This issue is patched in Tuleap Community Edition 14.0.99.24 and Tuleap Enterprise Edition 14.0-3. There are no known workarounds.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-5355	The Dell Isilon OneFS versions 8.2.2 and earlier SSHD process improperly allows Transmission Control Protocol (TCP) and stream forwarding. This provides the remotesupport user and users with restricted shells more access than is intended.	4.3	More Details
CVE-2022-43432	Jenkins XFramium Builder Plugin 1.0.22 and earlier programmatically disables Content-Security-Policy protection for user-generated content in workspaces, archived artifacts, etc. that Jenkins offers for download.	4.3	More Details
CVE-2022-27622	Server-Side Request Forgery (SSRF) vulnerability in Package Center functionality in Synology DiskStation Manager (DSM) before 7.1-42661 allows remote authenticated users to access intranet resources via unspecified vectors.	4.1	More Details
CVE-2022-39314	Kirby is a flat-file CMS. In versions prior to 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1, Kirby is subject to user enumeration due to Improper Restriction of Excessive Authentication Attempts. This vulnerability affects you only if you are using the `code` or `password-reset` auth method with the `auth.methods` option or if you have enabled the `debug` option in production. By using two or more IP addresses and multiple login attempts, valid user accounts will lock, but invalid accounts will not, leading to account enumeration. This issue has been patched in versions 3.5.8.2, 3.6.6.2, 3.7.5.1, and 3.8.1. If you cannot update immediately, you can work around the issue by setting the `auth.methods` option to `password`, which disables the code-based login and password reset forms.	3.7	More Details
CVE-2022-41983	On specific hardware platforms, on BIG-IP versions 16.1.x before 16.1.3.1, 15.1.x before 15.1.7, 14.1.x before 14.1.5.1, and all versions of 13.1.x, while Intel QAT (QuickAssist Technology) and the AES-GCM/CCM cipher is in use, undisclosed conditions can cause BIG-IP to send data unencrypted even with an SSL Profile applied.	3.7	More Details
CVE-2022-3606	A vulnerability was found in Linux Kernel. It has been classified as problematic. This affects the function find_prog_by_sec_insn of the file tools/lib/bpf/libbpf.c of the component BPF. The manipulation leads to null pointer dereference. It is recommended to apply a patch to fix this issue. The identifier VDB-211749 was assigned to this vulnerability.	3.5	More Details
CVE-2022-3633	A vulnerability classified as problematic has been found in Linux Kernel. Affected is the function j1939_session_destroy of the file net/can/j1939/transport.c. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211932.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3619	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function l2cap_recv_acldata of the file net/bluetooth/l2cap_core.c of the component Bluetooth. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. VDB-211918 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-3624	A vulnerability was found in Linux Kernel and classified as problematic. Affected by this issue is the function rlb_arp_xmit of the file drivers/net/bonding/bond_alb.c of the component IPsec. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211928.	3.5	More Details
CVE-2022-39259	jadx is a set of command line and GUI tools for producing Java source code from Android Dex and Apk files. versions prior to 1.4.5 are subject to a Denial of Service when opening zip files with HTML sequences. This issue has been patched in version 1.4.5. There are no known workarounds.	3.3	More Details
CVE-2022-3630	A vulnerability was found in Linux Kernel. It has been rated as problematic. This issue affects some unknown processing of the file fs/fscache/cookie.c of the component IPsec. The manipulation leads to memory leak. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-211931.	3.1	More Details
CVE-2022-3646	A vulnerability, which was classified as problematic, has been found in Linux Kernel. This issue affects the function nilfs_attach_log_writer of the file fs/nilfs2/segment.c of the component BPF. The manipulation leads to memory leak. The attack may be initiated remotely. It is recommended to apply a patch to fix this issue. The identifier VDB-211961 was assigned to this vulnerability.	3.1	More Details
CVE-2022-3647	** DISPUTED ** A vulnerability, which was classified as problematic, was found in Redis up to 6.2.7/7.0.5. Affected is the function sigsegvHandler of the file debug.c of the component Crash Report. The manipulation leads to denial of service. The complexity of an attack is rather high. The exploitability is told to be difficult. The real existence of this vulnerability is still doubted at the moment. Upgrading to version 6.2.8 and 7.0.6 is able to address this issue. The patch is identified as 0bf90d944313919eb8e63d3588bf63a367f020a3. It is recommended to apply a patch to fix this issue. VDB-211962 is the identifier assigned to this vulnerability. NOTE: The vendor claims that this is not a DoS because it applies to the crash logging mechanism which is triggered after a crash has occurred.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3649	A vulnerability was found in Linux Kernel. It has been classified as problematic. Affected is the function nilfs_new_inode of the file fs/nilfs2/inode.c of the component BPF. The manipulation leads to use after free. It is possible to launch the attack remotely. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211992.	3.1	More Details
CVE-2022-34845	A firmware update vulnerability exists in the sysupgrade functionality of Robustel R1510 3.1.16 and 3.3.0. A specially-crafted network packet can lead to arbitrary firmware update. An attacker can send a sequence of requests to trigger this vulnerability.	2.7	More Details
CVE-2022-3637	A vulnerability has been found in Linux Kernel and classified as problematic. This vulnerability affects the function jlink_init of the file monitor/jlink.c of the component BlueZ. The manipulation leads to denial of service. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-211936.	2.6	More Details
CVE-2022-3629	A vulnerability was found in Linux Kernel. It has been declared as problematic. This vulnerability affects the function vsock_connect of the file net/vmw_vsock/af_vsock.c. The manipulation leads to memory leak. The complexity of an attack is rather high. The exploitation appears to be difficult. It is recommended to apply a patch to fix this issue. VDB-211930 is the identifier assigned to this vulnerability.	2.6	More Details
CVE-2022-20424	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-2022-1970	Rejected reason: The originally reported issue in https://github.com/syedsohaibkarim/OpenRedirect-Keycloak18.0.0 is a known misconfiguration, and recommendation already exists in the Keycloak documentation to mitigate the issue: https://www.keycloak.org/docs/latest/server_admin/index.html#open-redirectors.	N/A	More Details
CVE-2022-3642	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-2022-3638	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 Number	Description	Base Score	Reference
CVE-2021-46849	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-29421. Reason: This candidate is a duplicate of CVE-2021-29421. Notes: All CVE users should reference CVE-2021-29421 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details