BULLETIN (SB22-052)

VULNERABILITY SUMMARY FOR THE WEEK OF

**28TH FEBRUARY, 2022**

# Bulletin (SB22-052)
# Vulnerability Summary for the Week of February 28, 2022

Cybernetic GI Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) / United States Computer Emergency Readiness Team, is sponsored by The NVD. For modified or updated entries, please visit the NVD, which contains historical vulnerability information.
The vulnerabilities are based on the CVE vulnerability naming standard and determined by the Common Vulnerability Scoring System (CVSS) standard. They are organized according to severity, by the division of high, medium and low severities correspond to the following scores:

High- Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0.
Medium - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0.6.9 -
Low - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9.

Entries may include additional information provided by organizations and efforts sponsored by Cybernetic GI. This data may include identifying information, values, definitions, and related links. The patch information is provided to users when available. Please note that some of the information in the bulletin is compiled from external, open source reports and is not a direct result of Cybernetic GI analysis .
The NCCIC Weekly Vulnerability Summary Bulletin is created using information from the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). In some cases, the vulnerabilities in the bulletin may not yet have assigned CVSS scores. Please visit NVD for updated vulnerability entries, which include CVSS scores once they are available.

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| \[gwa\]_autoresponder_project -- \[gwa\]_autoresponder | Unauthenticated SQL Injection (SQLi) vulnerability discovered in [GWA] AutoResponder WordPress plugin (versions <= 2.3), vulnerable at (&listid). No patched version available, plugin closed. | 2022-02-04 | 7.5 | CVE-2021-44779 |
| advantech -- adam-3600_firmware | The affected product has a hardcoded private key available inside the project folder, which may allow an attacker to achieve Web Server login and perform further actions. | 2022-02-04 | 7.5 | CVE-2022-22987 |
| apache -- gobblin | Apache Gobblin trusts all certificates used for LDAP connections in Gobblin-as-a-Service. This affects versions <= 0.15.0. Users should update to version 0.16.0 which addresses this issue. | 2022-02-04 | 7.5 | CVE-2021-36152 |
| debian -- perm | perM 0.4.0 has a Buffer Overflow related to strncpy. (Debian initially fixed this in 0.4.0-7.) | 2022-02-05 | 7.5 | CVE-2021-38172 |
| dlink -- di-7200g_v2_firmware | D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function proxy_client.asp. This vulnerability allows attackers to execute arbitrary commands via the proxy_srv, proxy_srvport, proxy_lanip, proxy_lanport parameters. | 2022-02-04 | 7.5 | CVE-2021-46227 |
| dlink -- di-7200g_v2_firmware | D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function usb_paswd.asp. This vulnerability allows attackers to execute arbitrary commands via the name parameter. | 2022-02-04 | 7.5 | CVE-2021-46229 |
| dlink -- di-7200g_v2_firmware | D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function msp_info.htm. This vulnerability allows attackers to execute arbitrary commands via the cmd parameter. | 2022-02-04 | 7.5 | CVE-2021-46233 |
| dlink -- di-7200g_v2_firmware | D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function version_upgrade.asp. This vulnerability allows attackers to execute arbitrary commands via the path parameter. | 2022-02-04 | 7.5 | CVE-2021-46232 |
| dlink -- di-7200g_v2_firmware | D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function urlrd_opt.asp. This vulnerability allows attackers to execute arbitrary commands via the url_en parameter. | 2022-02-04 | 7.5 | CVE-2021-46231 |
| dlink -- di-7200g_v2_firmware | D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function wget_test.asp. This vulnerability allows attackers to execute arbitrary commands via the url parameter. | 2022-02-04 | 7.5 | CVE-2021-46226 |
| dlink -- di-7200g_v2_firmware | D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function upgrade_filter. This vulnerability allows attackers to execute arbitrary commands via the path and time parameters. | 2022-02-04 | 7.5 | CVE-2021-46230 |
| dlink -- di-7200g_v2_firmware | D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a command injection vulnerability in the function httpd_debug.asp. This vulnerability allows attackers to execute arbitrary commands via the time parameter. | 2022-02-04 | 7.5 | CVE-2021-46228 |
| dlink -- dir-823_pro_firmware | D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function SetStationSettings. This vulnerability allows attackers to execute arbitrary commands via the station_access_enable parameter. | 2022-02-04 | 7.5 | CVE-2021-46455 |
| dlink -- dir-823_pro_firmware | D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function SetNetworkTomographySettings. This vulnerability allows attackers to execute arbitrary commands via the tomography_ping_address, tomography_ping_number, tomography_ping_size, tomography_ping_timeout, and tomography_ping_ttl parameters. | 2022-02-04 | 7.5 | CVE-2021-46452 |
| dlink -- dir-823_pro_firmware | D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function ChgSambaUserSettings. This vulnerability allows attackers to execute arbitrary commands via the samba_name parameter. | 2022-02-04 | 7.5 | CVE-2021-46457 |
| dlink -- dir-823_pro_firmware | D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function SetWLanACLSettings. This vulnerability allows attackers to execute arbitrary commands via the wl(0).(0)_maclist parameter. | 2022-02-04 | 7.5 | CVE-2021-46456 |
| dlink -- dir-823_pro_firmware | D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function SetStaticRouteSettings. This vulnerability allows attackers to execute arbitrary commands via the staticroute_list parameter. | 2022-02-04 | 7.5 | CVE-2021-46453 |
| dlink -- dir-823_pro_firmware | D-Link device D-Link DIR-823-Pro v1.0.2 was discovered to contain a command injection vulnerability in the function SetWLanApcliSettings. This vulnerability allows attackers to execute arbitrary commands via the ApCliKeyStr parameter. | 2022-02-04 | 7.5 | CVE-2021-46454 |
| dlink -- dir-878_firmware | D-Link devices DIR_878 DIR_878_FW1.30B08_Hotfix_02 and DIR_882 DIR_882_FW1.30B06_Hotfix_02 were discovered to contain a command injection vulnerability in the system function. This vulnerability allows attackers to execute arbitrary commands via a crafted HNAP1 POST request. | 2022-02-04 | 10 | CVE-2021-44880 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| dlink -- dir-878_firmware | D-Link device DIR_878_FW1.30B08_Hotfix_02 was discovered to contain a command injection vulnerability in the twsystem function. This vulnerability allows attackers to execute arbitrary commands via a crafted HNAP1 POST request. | 2022-02-04 | 10 | CVE-2021-44882 |
| dlink -- dir-882_firmware | D-Link device DIR_882 DIR_882_FW1.30B06_Hotfix_02 was discovered to contain a command injection vulnerability in the LocalIPAddress parameter. This vulnerability allows attackers to execute arbitrary commands via a crafted HNAP1 POST request. | 2022-02-04 | 7.5 | CVE-2021-45998 |
| dlink -- dir-882_firmware | D-Link device DIR_882 DIR_882_FW1.30B06_Hotfix_02 was discovered to contain a command injection vulnerability in the twsystem function. This vulnerability allows attackers to execute arbitrary commands via a crafted HNAP1 POST request. | 2022-02-04 | 10 | CVE-2021-44881 |
| emlog -- emlog | Emlog v6.0 was discovered to contain a SQL injection vulnerability via the $TagID parameter of getblogidsfromtagid(). | 2022-02-04 | 7.5 | CVE-2022-23379 |
| eset -- endpoint_antivirus | ESET products for Windows allows untrusted process to impersonate the client of a pipe, which can be leveraged by attacker to escalate privileges in the context of NT AUTHORITY\SYSTEM. | 2022-02-09 | 7.2 | CVE-2021-37852 |
| gitea -- gitea | Gitea before 1.11.2 is affected by Trusting HTTP Permission Methods on the Server Side when referencing the vulnerable admin or user API. which could let a remote malisious user execute arbitrary code. | 2022-02-08 | 7.5 | CVE-2021-45327 |
| globalnorthstar -- northstar_club_management | Systemic Insecure Permissions in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote unauthenticated users to use various functionalities without authentication. | 2022-02-04 | 7.5 | CVE-2021-29396 |
| globalnorthstar -- northstar_club_management | Remote Code Execution in cominput.jsp and comoutput.jsp in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote unauthenticated users to inject and execute arbitrary system commands via the unsanitized user-controlled "command" and "commandvalues" parameters. | 2022-02-04 | 10 | CVE-2021-29393 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. Under certain scenarios, Grappler component of TensorFlow is vulnerable to an integer overflow during cost estimation for crop and resize. Since the cropping parameters are user controlled, a malicious person can trigger undefined behavior. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 7.5 | CVE-2022-23587 |
| hyphp -- hybbs2 | Admin.php in HYBBS2 through 2.3.2 allows remote code execution because it writes plugin-related configuration information to conf.php. | 2022-02-09 | 7.5 | CVE-2022-24677 |
| idreamsoft -- icms | iCMS <= 8.0.0 allows users to add and render a comtom template, which has a SSTI vulnerability which causes remote code execution. | 2022-02-04 | 7.5 | CVE-2021-44978 |
| itunesrpc-remastered_project -- itunesrpc-remastered | iTunesRPC-Remastered is a Discord Rich Presence for iTunes on Windows utility. In affected versions iTunesRPC-Remastered did not properly sanitize image file paths leading to OS level command injection. This issue has been patched in commit cdcd48b. Users are advised to upgrade. | 2022-02-04 | 7.5 | CVE-2022-23611 |
| joplin_project -- joplin | Joplin 2.6.10 allows remote attackers to execute system commands through malicious code in user search results. | 2022-02-08 | 7.5 | CVE-2022-23340 |
| korenix -- jetwave_2212s_firmware | Certain Korenix JetWave devices allow authenticated users to execute arbitrary code as root via /syscmd.asp. This affects 2212X before 1.9.1, 2212S before 1.9.1, 2212G before 1.8, 3220 V3 before 1.5.1, 3420 V3 before 1.5.1, and 2311 through 2022-01-31. | 2022-02-06 | 9 | CVE-2021-39280 |
| linux -- linux_kernel | A use-after-free flaw was found in cgroup1_parse_param in kernel/cgroup/cgroup-v1.c in the Linux kernel's cgroup v1 parser. A local attacker with a user privilege could cause a privilege escalation by exploiting the fsconfig syscall parameter leading to a container breakout and a denial of service on the system. | 2022-02-04 | 7.2 | CVE-2021-4154 |
| mruby -- mruby | NULL Pointer Dereference in Homebrew mruby prior to 3.2. | 2022-02-04 | 7.8 | CVE-2022-0481 |
| nats -- nats_server | NATS nats-server before 2.7.2 has Incorrect Access Control. Any authenticated user can obtain the privileges of the System account by misusing the "dynamically provisioned sandbox accounts" feature. | 2022-02-08 | 9 | CVE-2022-24450 |
| neutrinolabs -- xrdp | xrdp is an open source remote desktop protocol (RDP) server. In affected versions an integer underflow leading to a heap overflow in the sesman server allows any unauthenticated attacker which is able to locally access a sesman server to execute code as root. This vulnerability has been patched in version 0.9.18.1 and above. Users are advised to upgrade. There are no known workarounds. | 2022-02-07 | 7.2 | CVE-2022-23613 |
| putil-merge_project -- putil-merge | This affects the package putil-merge before 3.8.0. The merge() function does not check the values passed into the argument. An attacker can supply a malicious value by adjusting the value to include the constructor property. Note: This | 2022-02-04 | 7.5 | CVE-2021-23470 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | vulnerability derives from an incomplete fix in https://security.snyk.io/vuln/SNYK-JS-PUTILMERGE-1317077 | | | |
| radare -- radare2 | Use After Free in GitHub repository radareorg/radare2 prior to 5.6.0. | 2022-02-08 | 7.5 | CVE-2022-0139 |
| riconmobile -- s9922l_firmware | The affected product is vulnerable to an authenticated OS command injection, which may allow an attacker to inject and execute arbitrary shell commands as the Admin (root) user. | 2022-02-04 | 10 | CVE-2022-0365 |
| sap -- content_server | SAP NetWeaver Application Server ABAP, SAP NetWeaver Application Server Java, ABAP Platform, SAP Content Server 7.53 and SAP Web Dispatcher are vulnerable for request smuggling and request concatenation. An unauthenticated attacker can prepend a victim's request with arbitrary data. This way, the attacker can execute functions impersonating the victim or poison intermediary Web caches. A successful attack could result in complete compromise of Confidentiality, Integrity and Availability of the system. | 2022-02-09 | 10 | CVE-2022-22536 |
| sap -- netweaver_application_server_java | In SAP NetWeaver Application Server Java - versions KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, an unauthenticated attacker could submit a crafted HTTP server request which triggers improper shared memory buffer handling. This could allow the malicious payload to be executed and hence execute functions that could be impersonating the victim or even steal the victim's logon session. | 2022-02-09 | 7.5 | CVE-2022-22532 |
| schneider-electric -- easergy_p3_firmware | A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted. Affected Product: Easergy P3 (All versions prior to V30.205) | 2022-02-04 | 8.3 | CVE-2022-22725 |
| schneider-electric -- easergy_p5_firmware | A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted. Affected Product: Easergy P5 (All firmware versions prior to V01.401.101) | 2022-02-04 | 8.3 | CVE-2022-22723 |
| schneider-electric -- ecostruxure_power_monitoring_expert | A CWE-20: Improper Input Validation vulnerability exists that could allow an unauthenticated attacker to view data, change settings, impact availability of the software, or potentially impact a user?s local machine when the user clicks a specially crafted link. Affected Product: EcoStruxure Power Monitoring Expert (Versions 2020 and prior) | 2022-02-04 | 9.3 | CVE-2022-22727 |
| sealevel -- seaconnect_370w_firmware | A stack-based buffer overflow vulnerability exists in both the LLMNR functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A specially-crafted network packet can lead to remote code execution. An attacker can send a malicious packet to trigger this vulnerability. | 2022-02-04 | 7.5 | CVE-2021-21960 |
| sealevel -- seaconnect_370w_firmware | A stack-based buffer overflow vulnerability exists in the NBNS functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A specially-crafted network packet can lead to remote code execution. An attacker can send a malicious packet to trigger this vulnerability. | 2022-02-04 | 7.5 | CVE-2021-21961 |
| sealevel -- seaconnect_370w_firmware | A denial of service vulnerability exists in the Modbus configuration functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. Specially-crafted network packets can lead to denial of service. An attacker can send a malicious packet to trigger this vulnerability. | 2022-02-04 | 7.1 | CVE-2021-21964 |
| servisnet -- tessa | An issue was discovered in Servisnet Tessa 0.0.2. Authorization data is available via an unauthenticated /data-service/users/ request. | 2022-02-06 | 10 | CVE-2022-22832 |
| servisnet -- tessa | An issue was discovered in Servisnet Tessa 0.0.2. An attacker can add a new sysadmin user via a manipulation of the Authorization HTTP header. | 2022-02-06 | 7.5 | CVE-2022-22831 |
| set_project -- set | This affects the package @strikeentco/set before 1.0.2. It allows an attacker to cause a denial of service and may lead to remote code execution. **Note:** This vulnerability derives from an incomplete fix in https://security.snyk.io/vuln/SNYK-JS-STRIKEENTCOSET-1038821 | 2022-02-04 | 7.5 | CVE-2021-23497 |
| silabs -- zgm130s037hgn_firmware | Z-Wave devices from Sierra Designs (circa 2013) and Silicon Labs (using S0 security) may use a known, shared network key of all zeros, allowing an attacker within radio range to spoof Z-Wave traffic. | 2022-02-04 | 7.9 | CVE-2013-20003 |
| skratchdot -- object-path-set | The package object-path-set before 1.0.2 are vulnerable to Prototype Pollution via the setPath method, as it allows an attacker to merge object prototypes into it. | 2022-02-04 | 7.5 | CVE-2021-23507 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | *Note:* This vulnerability derives from an incomplete fix in https://security.snyk.io/vuln/SNYK-JS-OBJECTPATHSET-607908 | | | |
| starwindsoftware -- iscsi_san | StarWind iSCSI SAN before 6.0 build 2013-03-20 allows a memory leak. | 2022-02-06 | 7.5 | CVE-2013-20004 |
| starwindsoftware -- nas | StarWind SAN and NAS before 0.2 build 1685 allows remote code execution via a virtual disk management command. | 2022-02-06 | 10 | CVE-2022-24552 |
| starwindsoftware -- nas | StarWind SAN and NAS before 0.2 build 1685 allows users to reset other users' passwords. | 2022-02-06 | 9 | CVE-2022-24551 |
| strangerstudios -- paid_memberships_pro | The Paid Memberships Pro WordPress plugin before 2.6.7 does not escape the discount_code in one of its REST route (available to unauthenticated users) before using it in a SQL statement, leading to a SQL injection | 2022-02-07 | 7.5 | CVE-2021-25114 |
| symfony -- twig | Twig is an open source template language for PHP. When in a sandbox mode, the `arrow` parameter of the `sort` filter must be a closure to avoid attackers being able to run arbitrary PHP functions. In affected versions this constraint was not properly enforced and could lead to code injection of arbitrary PHP code. Patched versions now disallow calling non Closure in the `sort` filter as is the case for some other filters. Users are advised to upgrade. | 2022-02-04 | 7.5 | CVE-2022-23614<br>FEDORA<br>FEDORA<br>FEDORA<br>FEDORA |
| synology -- diskstation_manager | Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Log Management functionality in Synology DiskStation Manager (DSM) before 7.0.1-42218-2 allows remote attackers to inject SQL commands via unspecified vectors. | 2022-02-07 | 7.5 | CVE-2021-43925 |
| synology -- diskstation_manager | Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Log Management functionality in Synology DiskStation Manager (DSM) before 7.0.1-42218-2 allows remote attackers to inject SQL commands via unspecified vectors. | 2022-02-07 | 7.5 | CVE-2021-43926 |
| synology -- diskstation_manager | Improper neutralization of special elements used in an SQL command ('SQL Injection') vulnerability in Security Management functionality in Synology DiskStation Manager (DSM) before 7.0.1-42218-2 allows remote attackers to inject SQL commands via unspecified vectors. | 2022-02-07 | 7.5 | CVE-2021-43927 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function WanParameterSetting. This vulnerability allows attackers to execute arbitrary commands via the gateway, dns1, and dns2 parameters. | 2022-02-04 | 7.5 | CVE-2022-24144 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetRouteStatic. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. | 2022-02-04 | 7.8 | CVE-2022-24152 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function mDMZSetCfg. This vulnerability allows attackers to execute arbitrary commands via the dmzIp parameter. | 2022-02-04 | 7.5 | CVE-2022-24148 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a command injection vulnerability in the function formSetSafeWanWebMan. This vulnerability allows attackers to execute arbitrary commands via the remoteIp parameter. | 2022-02-04 | 7.5 | CVE-2022-24150 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetFirewallCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via the firewallEn parameter. | 2022-02-04 | 7.8 | CVE-2022-24142 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formWifiBasicSet. This vulnerability allows attackers to cause a Denial of Service (DoS) via the security and security_5g parameters. | 2022-02-04 | 7.8 | CVE-2022-24145 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetQosBand. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. | 2022-02-04 | 7.8 | CVE-2022-24146 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromAdvSetMacMtuWan. This vulnerability allows attackers to cause a Denial of Service (DoS) via the wanMTU, wanSpeed, cloneType, mac, and serviceName parameters. | 2022-02-04 | 7.8 | CVE-2022-24147 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetWirelessRepeat. This vulnerability allows attackers to cause a Denial of Service (DoS) via the wpapsk_crypto parameter. | 2022-02-04 | 7.8 | CVE-2022-24149 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetWifiGusetBasic. This vulnerability allows attackers to cause a Denial of Service (DoS) via the shareSpeed parameter. | 2022-02-04 | 7.8 | CVE-2022-24151 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN and AX12 22.03.01.2_CN was discovered to contain a stack overflow in the function form_fast_setting_wifi_set. This vulnerability allows attackers to cause a Denial of Service (DoS) via the timeZone parameter. | 2022-02-04 | 7.8 | CVE-2022-24143 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formAddMacfilterRule. This vulnerability allows attackers to cause a Denial of Service (DoS) via the devName parameter. | 2022-02-04 | 7.8 | CVE-2022-24153 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetMacFilterCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via the deviceList parameter. | 2022-02-04 | 7.8 | CVE-2022-24157 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetDeviceName. This vulnerability allows attackers to cause a Denial of Service (DoS) via the devName parameter. | 2022-02-04 | 7.8 | CVE-2022-24160 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetIpMacBind. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. | 2022-02-04 | 7.8 | CVE-2022-24158 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a heap overflow in the function GetParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the mac parameter. | 2022-02-04 | 7.8 | CVE-2022-24161 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function saveParentControlInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the time parameter. | 2022-02-04 | 7.8 | CVE-2022-24162 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetRebootTimer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the rebootTime parameter. | 2022-02-04 | 7.8 | CVE-2022-24154 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetPPTPServer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the startIp and endIp parameters. | 2022-02-04 | 7.8 | CVE-2022-24159 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function formSetVirtualSer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the list parameter. | 2022-02-04 | 7.8 | CVE-2022-24156 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a stack overflow in the function fromSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the timeZone parameter. | 2022-02-04 | 7.8 | CVE-2022-24163 |
| tenda -- ax3_firmware | Tenda AX3 v16.03.12.10_CN was discovered to contain a heap overflow in the function setSchedWifi. This vulnerability allows attackers to cause a Denial of Service (DoS) via the schedStartTime and schedEndTime parameters. | 2022-02-04 | 7.8 | CVE-2022-24155 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetPppoeServer. This vulnerability allows attackers to execute arbitrary commands via the pppoeServerIP, pppoeServerStartIP, and pppoeServerEndIP parameters. | 2022-02-04 | 7.5 | CVE-2022-24171 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpGroup. This vulnerability allows attackers to execute arbitrary commands via the IPGroupStartIP and IPGroupEndIP parameters. | 2022-02-04 | 7.5 | CVE-2022-24168 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetDMZ. This vulnerability allows attackers to execute arbitrary commands via the dmzHost1 parameter. | 2022-02-04 | 7.5 | CVE-2022-24167 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetQvlanList. This vulnerability allows attackers to execute arbitrary commands via the qvlanIP parameter. | 2022-02-04 | 7.5 | CVE-2022-24165 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetVirtualSer. This vulnerability allows attackers to cause a Denial of Service (DoS) via the DnsHijackRule parameter. | 2022-02-04 | 7.8 | CVE-2022-24164 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetSysTime. This vulnerability allows attackers to cause a Denial of Service (DoS) via the manualTime parameter. | 2022-02-04 | 7.8 | CVE-2022-24166 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetIpSecTunnel. This vulnerability allows attackers to execute arbitrary commands via the IPsecLocalNet and IPsecRemoteNet parameters. | 2022-02-04 | 7.5 | CVE-2022-24170 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formAddDnsForward. This vulnerability allows attackers to cause a Denial of Service (DoS) via the DnsForwardRule parameter. | 2022-02-04 | 7.8 | CVE-2021-45988 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function guestWifiRuleRefresh. This vulnerability allows attackers to cause a Denial of Service (DoS) via the qosGuestUpstream and qosGuestDownstream parameters. | 2022-02-04 | 7.8 | CVE-2021-45989 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetStaticRoute. This vulnerability allows attackers to cause a Denial of Service (DoS) via the staticRouteNet, staticRouteMask, and staticRouteGateway parameters. | 2022-02-04 | 7.8 | CVE-2021-45995 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function uploadPicture. This vulnerability allows attackers to execute arbitrary commands via the pic_name parameter. | 2022-02-04 | 7.5 | CVE-2021-45990 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetNetCheckTools. This vulnerability allows attackers to execute arbitrary commands via the hostName parameter. | 2022-02-04 | 7.5 | CVE-2021-45987 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a command injection vulnerability in the function formSetUSBShareInfo. This vulnerability allows attackers to execute arbitrary commands via the usbOrdinaryUserName parameter. | 2022-02-04 | 7.5 | CVE-2021-45986 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formAddDhcpBindRule. This vulnerability allows attackers to cause a Denial of Service (DoS) via the addDhcpRules parameter. | 2022-02-04 | 7.8 | CVE-2022-24172 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetPortMapping. This vulnerability allows attackers to cause a Denial of Service (DoS) via the portMappingServer, portMappingProtocol, portMappingWan, porMappingtInternal, and portMappingExternal parameters. | 2022-02-04 | 7.8 | CVE-2021-45997 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetPortMapping. This vulnerability allows attackers to cause a Denial of Service (DoS) via the portMappingServer, portMappingProtocol, portMappingWan, porMappingtInternal, and portMappingExternal parameters. | 2022-02-04 | 7.8 | CVE-2021-45996 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formDelDhcpRule. This vulnerability allows attackers to cause a Denial of Service (DoS) via the delDhcpIndex parameter. | 2022-02-04 | 7.8 | CVE-2021-45994 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formIPMacBindModify. This vulnerability allows attackers to cause a Denial of Service (DoS) via the IPMacBindRuleIP and IPMacBindRuleMac parameters. | 2022-02-04 | 7.8 | CVE-2021-45993 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formSetQvlanList. This vulnerability allows attackers to cause a Denial of Service (DoS) via the qvlanName parameter. | 2022-02-04 | 7.8 | CVE-2021-45992 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formAddVpnUsers. This vulnerability allows attackers to cause a Denial of Service (DoS) via the vpnUsers parameter. | 2022-02-04 | 7.8 | CVE-2021-45991 |
| tendacn -- g1_firmware | Tenda routers G1 and G3 v15.11.0.17(9502)_CN were discovered to contain a stack overflow in the function formIPMacBindAdd. This vulnerability allows attackers to cause a Denial of Service (DoS) via the IPMacBindRule parameter. | 2022-02-04 | 7.8 | CVE-2022-24169 |
| totolink -- a720r_firmware | Totolink devices A3100R v4.1.2cu.5050_B20200504, A830R v5.9c.4729_B20191112, and A720R v4.1.5cu.470_B20200911 were discovered to contain a stack overflow in the function setNoticeCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via the IpTo parameter. | 2022-02-04 | 7.8 | CVE-2021-44246 |
| totolink -- a720r_firmware | Totolink devices A3100R v4.1.2cu.5050_B20200504, A830R v5.9c.4729_B20191112, and A720R v4.1.5cu.470_B20200911 were discovered to contain command injection vulnerability in the function setNoticeCfg. This vulnerability allows attackers to execute arbitrary commands via the IpFrom parameter. | 2022-02-04 | 7.5 | CVE-2021-44247 |
| ujcms -- jspxcms | A vulnerability in ${"freemarker.template.utility.Execute"?new() of UJCMS Jspxcms v10.2.0 allows attackers to execute arbitrary commands via uploading malicious files. | 2022-02-04 | 7.5 | CVE-2022-23329 |
| voipmonitor -- voipmonitor | An incorrect check in the component cdr.php of Voipmonitor GUI before v24.96 allows unauthenticated attackers to escalate privileges via a crafted request. | 2022-02-04 | 7.5 | CVE-2022-24259 |
| voipmonitor -- voipmonitor | A SQL injection vulnerability in Voipmonitor GUI before v24.96 allows attackers to escalate privileges to the Administrator level. | 2022-02-04 | 10 | CVE-2022-24260 |
| zephyrproject -- zephyr | The RNDIS USB device class includes a buffer overflow vulnerability. Zephyr versions >= v2.6.0 contain Heap-based Buffer Overflow (CWE-122). For more | 2022-02-07 | 7.2 | CVE-2021-3861 N/A |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-hvfp-w4h8-gxvj | | | |
| accel-ppp -- accel-ppp | The rad_packet_recv function in opt/src/accel-pppd/radius/packet.c suffers from a buffer overflow vulnerability, whereby user input len is copied into a fixed buffer &attr->val.integer without any bound checks. If the client connects to the server and sends a large radius packet, a buffer overflow vulnerability will be triggered. | 2022-02-14 | 7.5 | CVE-2022-24704 |
| accel-ppp -- accel-ppp | The rad_packet_recv function in radius/packet.c suffers from a memcpy buffer overflow, resulting in an overly-large recvfrom into a fixed buffer that causes a buffer overflow and overwrites arbitrary memory. If the server connects with a malicious client, crafted client requests can remotely trigger this vulnerability. | 2022-02-14 | 7.5 | CVE-2022-24705 |
| apache -- apisix | An attacker can abuse the batch-requests plugin to send requests to bypass the IP restriction of Admin API. A default configuration of Apache APISIX (with default API key) is vulnerable to remote code execution. When the admin key was changed or the port of Admin API was changed to a port different from the data panel, the impact is lower. But there is still a risk to bypass the IP restriction of Apache APISIX's data panel. There is a check in the batch-requests plugin which overrides the client IP with its real remote IP. But due to a bug in the code, this check can be bypassed. | 2022-02-11 | 7.5 | CVE-2022-24112 MLIST |
| apache -- cassandra | When running Apache Cassandra with the following configuration: enable_user_defined_functions: true enable_scripted_user_defined_functions: true enable_user_defined_functions_threads: false it is possible for an attacker to execute arbitrary code on the host. The attacker would need to have enough permissions to create user defined functions in the cluster to be able to exploit this. Note that this configuration is documented as unsafe, and will continue to be considered unsafe after this CVE. | 2022-02-11 | 8.5 | CVE-2021-44521 MLIST |
| broadcom -- xcom_data_transport | XCOM Data Transport for Windows, Linux, and UNIX 11.6 releases contain a vulnerability due to insufficient input validation that could potentially allow remote attackers to execute arbitrary commands with elevated privileges. | 2022-02-14 | 10 | CVE-2022-23992 |
| dairy_farm_shop_management_system_project -- dairy_farm_shop_management_system | Dairy Farm Shop Management System v1.0 was discovered to contain hardcoded credentials in the source code which allows attackers access to the control panel if compromised. | 2022-02-11 | 7.5 | CVE-2020-36062 |
| drupal -- drupal | Drupal's JSON:API and REST/File modules allow file uploads through their HTTP APIs. The modules do not correctly run all file validation, which causes an access bypass vulnerability. An attacker might be able to upload files that bypass the file validation process implemented by modules on the site. | 2022-02-11 | 7.5 | CVE-2020-13675 |
| foxit -- pdf_reader | Foxit PDF Reader before 11.2.1 and Foxit PDF Editor before 11.2.1 have a Stack-Based Buffer Overflow related to XFA, for the 'subform colSpan="-2"' and 'draw colSpan="1"' substrings. | 2022-02-11 | 7.5 | CVE-2022-24954 |
| foxit -- pdf_reader | Foxit PDF Reader before 11.2.1 and Foxit PDF Editor before 11.2.1 have an Uncontrolled Search Path Element for DLL files. | 2022-02-11 | 7.5 | CVE-2022-24955 |
| golang -- go | Rat.SetString in math/big in Go before 1.16.14 and 1.17.x before 1.17.7 has an overflow that can lead to Uncontrolled Memory Consumption. | 2022-02-11 | 7.8 | CVE-2022-23772 |
| google -- android | In onActivityViewReady of DetailDialog.kt, there is a possible Intent Redirect due to a confused deputy. This could lead to local escalation of privilege that allows actions performed as the System UI, with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-193445603 | 2022-02-11 | 7.2 | CVE-2021-39668 |
| google -- android | In fastboot, there is a possible secure boot bypass due to a configuration error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android SoC Android ID: A-202018701 | 2022-02-11 | 7.2 | CVE-2021-39672 |
| google -- android | In openFileAndEnforcePathPermissionsHelper of MediaProvider.java, there is a possible bypass of a permissions check due to a confused deputy. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-200682135 | 2022-02-11 | 7.2 | CVE-2021-39663 |
| google -- android | In btm_sec_connected and btm_sec_disconnected of btm_sec.cc file , there is a possible use after free. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-201083442 | 2022-02-11 | 7.2 | CVE-2021-39674 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- android | In checkUriPermission of MediaProvider.java , there is a possible way to gain access to the content of media provider collections due to a missing permission check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-197302116 | 2022-02-11 | 7.2 | CVE-2021-39662 |
| google -- android | In updatePackageMappingsData of UsageStatsService.java, there is a possible way to bypass security and privacy settings of app usage due to an unusual root cause. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-197399948 | 2022-02-11 | 7.2 | CVE-2021-39619 |
| google -- android | In writeThrowable of AndroidFuture.java, there is a possible parcel serialization/deserialization mismatch due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-197228210 | 2022-02-11 | 7.2 | CVE-2021-39676 |
| google -- android | Summary:Product: AndroidVersions: Android SoCAndroid ID: A-204686438 | 2022-02-11 | 10 | CVE-2021-39616 |
| google -- android | An improper boundary check in eden_runtime hal service prior to SMR Feb-2022 Release 1 allows arbitrary memory write and code execution. | 2022-02-11 | 7.2 | CVE-2022-23428 |
| google -- android | In GKI_getbuf of gki_buffer.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-205729183 | 2022-02-11 | 10 | CVE-2021-39675 |
| google -- android | ismsEx service is a vendor service in unisoc equipment?ismsEx service is an extension of sms system service?but it does not check the permissions of the caller?resulting in permission leaks?Third-party apps can use this service to arbitrarily modify and set system properties?Product: AndroidVersions: Android SoCAndroid ID: A-207479207 | 2022-02-11 | 10 | CVE-2021-39658 |
| google -- android | Improper input validation in Exynos baseband prior to SMR Feb-2022 Release 1 allows attackers to send arbitrary NAS signaling messages with fake base station. | 2022-02-11 | 7.5 | CVE-2022-23425 |
| google -- android | ims_ex is a vendor system service used to manage VoLTE in unisoc devices?But it does not verify the caller's permissions?so that normal apps (No phone permissions) can obtain some VoLTE sensitive information and manage VoLTE calls.Product: AndroidVersions: Android SoCAndroid ID: A-206492634 | 2022-02-11 | 9.4 | CVE-2021-39635 |
| microweber -- microweber | OS Command Injection in Packagist microweber/microweber prior to 1.2.11. | 2022-02-11 | 9.3 | CVE-2022-0557 |
| mitsubishielectric -- cw_configurator | Multiple Mitsubishi Electric Factory Automation products have a vulnerability that allows an attacker to execute arbitrary code. | 2022-02-11 | 7.5 | CVE-2020-14523 |
| nokia -- bts_trs_web_console | Nokia BTS TRS web console FTM_W20_FP2_2019.08.16_0010 allows Authentication Bypass. A malicious unauthenticated user can get access to all the functionalities exposed via the web panel, circumventing the authentication process, by using URL encoding for the . (dot) character. | 2022-02-11 | 7.5 | CVE-2021-31932 |
| portainer -- portainer | In Portainer Agent before 2.11.1, an API server can continue running even if not associated with a Portainer instance in the past few days. | 2022-02-11 | 7.5 | CVE-2022-24961 |
| qualcomm -- apq8009w_firmware | Improper validation of maximum size of data write to EFS file can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables | 2022-02-11 | 7.2 | CVE-2021-30323 |
| qualcomm -- apq8096au_firmware | Improper validation of data length received from DMA buffer can lead to memory corruption. in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking | 2022-02-11 | 7.2 | CVE-2021-35069 |
| qualcomm -- aqt1000_firmware | Improper validation of program headers containing ELF metadata can lead to image verification bypass in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking | 2022-02-11 | 7.2 | CVE-2021-30317 |
| qualcomm -- aqt1000_firmware | Possible out of bounds write due to improper validation of number of GPIOs configured in an internal parameters array in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile | 2022-02-11 | 7.2 | CVE-2021-30322 |

# High Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| qualcomm -- ar8035_firmware | Possible integer overflow due to improper fragment datatype while calculating number of fragments in a request message in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile | 2022-02-11 | 7.2 | CVE-2021-35074 |
| qualcomm -- ar8035_firmware | Possible use after free scenario in compute offloads to DSP while multiple calls spawn a dynamic process in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile | 2022-02-11 | 7.2 | CVE-2021-35077 |
| qualcomm -- ar8035_firmware | Possible null pointer dereference due to lack of WDOG structure validation during registration in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile | 2022-02-11 | 7.2 | CVE-2021-35075 |
| radare -- radare2 | Use After Free in GitHub repository radareorg/radare2 prior to 5.6.2. | 2022-02-16 | 7.5 | CVE-2022-0559 |
| schneider-electric -- interactive_graphical_scada_system_data_collector | A CWE-434: Unrestricted Upload of File with Dangerous Type vulnerability exists that could lead to remote code execution through a number of paths, when an attacker, writes arbitrary files to folders in context of the DC module, by sending constructed messages on the network. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21243 and prior) | 2022-02-11 | 7.5 | CVE-2021-22803 |
| schneider-electric -- interactive_graphical_scada_system_data_collector | A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could result in remote code execution due to missing length check on user supplied data, when a constructed message is received on the network. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21243 and prior) | 2022-02-11 | 7.5 | CVE-2021-22802 |
| snowsoftware -- snow_inventory_java_scanner | A vulnerability in Snow Inventory Java Scanner allows an attacker to run malicious code at a higher level of privileges. This issue affects: SNOW Snow Inventory Java Scanner 1.0 | 2022-02-16 | 7.2 | CVE-2021-4106 |
| tongda2000 -- tongda_oa | Tongda2000 v11.10 was discovered to contain a SQL injection vulnerability in /mobile_seal/get_seal.php via the DEVICE_LIST parameter. | 2022-02-14 | 7.5 | CVE-2022-24206 |
| tongda2000 -- tongda_oa | Tongda2000 v11.10 was discovered to contain a SQL injection vulnerability in export_data.php via the d_name parameter. | 2022-02-14 | 7.5 | CVE-2022-23902 |
| tsg-solutions -- tokheim_profleet_dialog | Tokheim Profleet DiaLOG 11.005.02 is affected by SQL Injection. The component is the Field__UserLogin parameter on the logon page. | 2022-02-11 | 10 | CVE-2021-34235 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| abb -- opc_server_for_ac_800m | Incorrect Permission Assignment for Critical Resource vulnerability in OPC Server for AC 800M allows an attacker to execute arbitrary code in the node running the AC800M OPC Server. | 2022-02-04 | 6.5 | CVE-2021-22284 |
| abb -- pni800_firmware | Improper Input Validation vulnerability in the ABB SPIET800 and PNI800 module allows an attacker to cause the denial of service or make the module unresponsive. | 2022-02-04 | 5 | CVE-2021-22286 |
| abb -- pni800_firmware | Improper Handling of Exceptional Conditions, Improper Check for Unusual or Exceptional Conditions vulnerability in the ABB SPIET800 and PNI800 module that allows an attacker to cause the denial of service or make the module unresponsive. | 2022-02-04 | 5 | CVE-2021-22285 |
| abb -- pni800_firmware | Improper Input Validation vulnerability in the ABB SPIET800 and PNI800 module allows an attacker to cause the denial of service or make the module unresponsive. | 2022-02-04 | 5 | CVE-2021-22288 |
| acronis -- agent | Local privilege escalation due to excessive permissions assigned to child processes. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27147, Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287 | 2022-02-04 | 4.6 | CVE-2022-24113 |
| acronis -- true_image | Local privilege escalation via named pipe due to improper access control checks. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 28035, Acronis Agent (Windows) before build 27147, Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287 | 2022-02-04 | 4.6 | CVE-2021-44204 |
| acronis -- true_image | Local privilege escalation due to DLL hijacking vulnerability in Acronis Media Builder service. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287 | 2022-02-04 | 4.4 | CVE-2021-44206 |
| acronis -- true_image | Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 39612, Acronis True Image 2021 (Windows) before build 39287 | 2022-02-04 | 4.4 | CVE-2021-44205 |
| acronis -- true_image | Local privilege escalation due to unrestricted loading of unsigned libraries. The following products are affected: Acronis Cyber Protect Home Office (macOS) before build 39605, Acronis True Image 2021 (macOS) before build 39287 | 2022-02-04 | 4.6 | CVE-2022-24115 |
| acronis -- true_image | Local privilege escalation due to race condition on application startup. The following products are affected: Acronis Cyber Protect Home Office (macOS) before build 39605, Acronis True Image 2021 (macOS) before build 39287 | 2022-02-04 | 4.4 | CVE-2022-24114 |
| amd -- radeon_pro_software | AMD Radeon Software may be vulnerable to DLL Hijacking through path variable. An unprivileged user may be able to drop its malicious DLL file in any location which is in path environment variable. | 2022-02-04 | 4.4 | CVE-2020-12891 |
| amd -- ryzen_pro_5650g_firmware | When combined with specific software sequences, AMD CPUs may transiently execute non-canonical loads and store using only the lower 48 address bits potentially resulting in data leakage. | 2022-02-04 | 5 | CVE-2020-12965 |
| apache -- activemq_artemis | In Apache ActiveMQ Artemis prior to 2.20.0 or 2.19.1, an attacker could partially disrupt availability (DoS) through uncontrolled resource consumption of memory. | 2022-02-04 | 5 | CVE-2022-23913 |
| apache -- traffic_control | In Apache Traffic Control Traffic Ops prior to 6.1.0 or 5.1.6, an unprivileged user who can reach Traffic Ops over HTTPS can send a specially-crafted POST request to /user/login/oauth to scan a port of a server that Traffic Ops can reach. | 2022-02-06 | 5 | CVE-2022-23206 |
| arangodb -- arangodb | In ArangoDB, versions v3.7.0 through v3.9.0-alpha.1 have a feature which allows downloading a Foxx service from a publicly available URL. This feature does not enforce proper filtering of requests performed internally, which can be abused by a | 2022-02-09 | 4 | CVE-2021-25939 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | highly-privileged attacker to perform blind SSRF and send internal requests to localhost. | | | |
| arista -- eos | The impact of this vulnerability is that Arista's EOS eAPI may skip re-evaluating user credentials when certificate based authentication is used, which allows remote attackers to access the device via eAPI. | 2022-02-04 | 6.8 | CVE-2021-28503 |
| atftp_project -- atftp | options.c in atftp before 0.7.5 reads past the end of an array, and consequently discloses server-side /etc/group data to a remote client. | 2022-02-04 | 5 | CVE-2021-46671 |
| beanstalk_console_project -- beanstalk_console | Cross-site Scripting (XSS) - Reflected in Packagist ptrofimov/beanstalk_console prior to 1.7.12. | 2022-02-05 | 4.3 | CVE-2022-0501 |
| blog_project -- blog | m1k1o/blog is a lightweight self-hosted facebook-styled PHP blog. Errors from functions `imagecreatefrom*` and `image*` have not been checked properly. Although PHP issued warnings and the upload function returned `false`, the original file (that could contain a malicious payload) was kept on the disk. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue. | 2022-02-08 | 6.5 | CVE-2022-23626 |
| bracketspace -- advanced_cron_manager | The Advanced Cron Manager WordPress plugin before 2.4.2, advanced-cron-manager-pro WordPress plugin before 2.5.3 does not have authorisation checks in some of its AJAX actions, allowing any authenticated users, such as subscriber to call them and add or remove events as well as schedules for example | 2022-02-07 | 4 | CVE-2021-25084 |
| broadcom -- ca_harvest_software_change_manager | CA Harvest Software Change Manager versions 13.0.3, 13.0.4, 14.0.0, and 14.0.1, contain a vulnerability in the CSV export functionality, due to insufficient input validation, that can allow a privileged user to potentially execute arbitrary code or commands. | 2022-02-04 | 6.5 | CVE-2022-22689 |
| chatwoot -- chatwoot | Cross-site Scripting (XSS) - Stored in GitHub repository chatwoot/chatwoot prior to 2.2.0. | 2022-02-09 | 4.3 | CVE-2022-0527 |
| chatwoot -- chatwoot | Improper Privilege Management in GitHub repository chatwoot/chatwoot prior to v2.2. | 2022-02-09 | 4 | CVE-2021-3813 |
| chatwoot -- chatwoot | Cross-site Scripting (XSS) - Stored in GitHub repository chatwoot/chatwoot prior to 2.2.0. | 2022-02-09 | 4.3 | CVE-2022-0526 |
| codemiq -- wordpress_email_template_designer | The WP HTML Mail WordPress plugin is vulnerable to unauthorized access which allows unauthenticated attackers to retrieve and modify theme settings due to a missing capability check on the /themesettings REST-API endpoint found in the ~/includes/class-template-designer.php file, in versions up to and including 3.0.9. This makes it possible for attackers with no privileges to execute the endpoint and add malicious JavaScript to a vulnerable WordPress site. | 2022-02-04 | 4.3 | CVE-2022-0218 |
| codex_project -- codex | A Cross Site Scripting (XSS) vulnerability exists in Codex before 1.4.0 via Notebook/Page name field, which allows malicious users to execute arbitrary code via a crafted http code in a .json file. | 2022-02-04 | 4.3 | CVE-2021-43635 |
| dataease_project -- dataease | In DataEase v1.6.1, an authenticated user can gain unauthorized access to all user information and can change the administrator password. | 2022-02-08 | 6.5 | CVE-2022-23331 |
| dounokouno -- transmitmail | Cross-site scripting vulnerability in TransmitMail 2.5.0 to 2.6.1 allows a remote unauthenticated attacker to inject an arbitrary script via unspecified vectors. | 2022-02-08 | 4.3 | CVE-2022-22146 |
| dounokouno -- transmitmail | Directory traversal vulnerability in TransmitMail 2.5.0 to 2.6.1 allows a remote unauthenticated attacker to obtain an arbitrary file on the server via unspecified vectors. | 2022-02-08 | 5 | CVE-2022-21193 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| econosys-system -- php_mailform | Reflected cross-site scripting vulnerability in the checkbox of php_mailform versions prior to Version 1.40 allows a remote unauthenticated attacker to inject an arbitrary script via unspecified vectors. | 2022-02-08 | 4.3 | CVE-2022-22142 |
| econosys-system -- php_mailform | Reflected cross-site scripting vulnerability in the attached file name of php_mailform versions prior to Version 1.40 allows a remote unauthenticated attacker to inject an arbitrary script via unspecified vectors. | 2022-02-08 | 4.3 | CVE-2022-21805 |
| embed_swagger_project -- embed_swagger | The Embed Swagger WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient escaping/sanitization and validation via the url parameter found in the ~/swagger-iframe.php file which allows attackers to inject arbitrary web scripts onto the page, in versions up to and including 1.0.0. | 2022-02-04 | 4.3 | CVE-2022-0381 |
| etoilewebdesign -- ultimate_product_catalog | The Ultimate Product Catalog WordPress plugin before 5.0.26 does not have authorisation and CSRF checks in some AJAX actions, which could allow any authenticated users, such as subscriber to call them and add arbitrary products, or change the plugin's settings for example | 2022-02-07 | 4 | CVE-2021-24993 |
| f-secure -- atlant | A vulnerability affecting F-Secure antivirus engine before Capricorn update 2022-02-01_01 was discovered whereby decompression of ACE file causes the scanner service to stop. The vulnerability can be exploited remotely by an attacker. A successful attack will result in denial-of-service of the antivirus engine. | 2022-02-09 | 5 | CVE-2021-40837 |
| ffjpeg_project -- ffjpeg | Two Heap based buffer overflow vulnerabilities exist in ffjpeg through 01.01.2021. It is similar to CVE-2020-23852. Issues that are in the jfif_decode function at ffjpeg/src/jfif.c (line 552) could cause a Denial of Service by using a crafted jpeg file. | 2022-02-08 | 4.3 | CVE-2021-44956 |
| ffjpeg_project -- ffjpeg | Global buffer overflow vulnerability exist in ffjpeg through 01.01.2021. It is similar to CVE-2020-23705. Issue is in the jfif_encode function at ffjpeg/src/jfif.c (line 708) could cause a Denial of Service by using a crafted jpeg file. | 2022-02-08 | 4.3 | CVE-2021-44957 |
| filebrowser -- filebrowser | A Cross-Site Request Forgery vulnerability exists in Filebrowser < 2.18.0 that allows attackers to create a backdoor user with admin privilege and get access to the filesystem via a malicious HTML webpage that is sent to the victim. An admin can run commands using the FileBrowser and hence it leads to RCE. | 2022-02-04 | 6.8 | CVE-2021-46398 |
| fisco-bcos -- fisco-bcos | FISCO-BCOS release-3.0.0-rc2 contains a denial of service vulnerability. Some transactions may not be committed successfully, and malicious users may use this to achieve double-spending attacks. | 2022-02-07 | 5 | CVE-2021-46359 |
| follow-redirects_project -- follow-redirects | Exposure of Sensitive Information to an Unauthorized Actor in NPM follow-redirects prior to 1.14.8. | 2022-02-09 | 4.3 | CVE-2022-0536 |
| fotobook_project -- fotobook | The Fotobook WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to insufficient escaping and the use of $_SERVER['PHP_SELF'] found in the ~/options-fotobook.php file which allows attackers to inject arbitrary web scripts onto the page, in versions up to and including 3.2.3. | 2022-02-04 | 4.3 | CVE-2022-0380 |
| foxit -- pdf_reader | A use-after-free vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 11.1.0.52543. A specially-crafted PDF document can trigger the reuse of previously freed memory, which can lead to arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled. | 2022-02-04 | 6.8 | CVE-2021-40420 |
| foxit -- pdf_reader | A memory corruption vulnerability exists in the JavaScript engine of Foxit Software's PDF Reader, version 11.1.0.52543. A specially-crafted PDF document can trigger an exception which is improperly handled, leaving the engine in an invalid state, which can lead to memory corruption and arbitrary code execution. An attacker needs to trick the user to open the malicious file to trigger this | 2022-02-04 | 6.8 | CVE-2022-22150 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled. | | | |
| frourio -- frourio | Frourio is a full stack framework, for TypeScript. Frourio users who uses frourio version prior to v0.26.0 and integration with class-validator through `validators/` folder are subject to a input validation vulnerability. Validators do not work properly for request bodies and queries in specific situations and some input is not validated at all. Users are advised to update frourio to v0.26.0 or later and to install `class-transformer` and `reflect-metadata`. | 2022-02-07 | 6.5 | CVE-2022-23623 |
| frourio -- frourio-express | Frourio-express is a minimal full stack framework, for TypeScript. Frourio-express users who uses frourio-express version prior to v0.26.0 and integration with class-validator through `validators/` folder are subject to a input validation vulnerability. Validators do not work properly for request bodies and queries in specific situations and some input is not validated at all. Users are advised to update frourio to v0.26.0 or later and to install `class-transformer` and `reflect-metadata`. | 2022-02-07 | 6.5 | CVE-2022-23624 |
| gerbv_project -- gerbv | A use-after-free vulnerability exists in the RS-274X aperture definition tokenization functionality of Gerbv 2.7.0 and dev (commit b5f1eacd) and Gerbv forked 2.7.1. A specially-crafted gerber file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability. | 2022-02-04 | 6.8 | CVE-2021-40401 |
| gerbv_project -- gerbv | An information disclosure vulnerability exists in the pick-and-place rotation parsing functionality of Gerbv 2.7.0 and dev (commit b5f1eacd), and Gerbv forked 2.8.0. A specially-crafted pick-and-place file can exploit the missing initialization of a structure to leak memory contents. An attacker can provide a malicious file to trigger this vulnerability. | 2022-02-04 | 4.3 | CVE-2021-40403 |
| gitea -- gitea | Gitea before 1.4.3 is affected by URL Redirection to Untrusted Site ('Open Redirect') via internal URLs. | 2022-02-08 | 5.8 | CVE-2021-45328 |
| gitea -- gitea | Server Side Request Forgery (SSRF) vulneraility exists in Gitea before 1.7.0 using the OpenID URL. | 2022-02-08 | 5 | CVE-2021-45325 |
| gitea -- gitea | Cross Site Scripting (XSS) vulnerability exists in Gitea before 1.5.1 via the repository settings inside the external wiki/issue tracker URL field. | 2022-02-08 | 4.3 | CVE-2021-45329 |
| gitea -- gitea | Cross Site Request Forgery (CSRF) vulnerability exists in Gitea before 1.5.2 via API routes.This can be dangerous especially with state altering POST requests. | 2022-02-08 | 6.8 | CVE-2021-45326 |
| globalnorthstar -- northstar_club_management | Directory travesal in /northstar/filemanager/download.jsp in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote unauthenticated users to download arbitrary files, including JSP source code, across the filesystem of the host of the web application. | 2022-02-04 | 5 | CVE-2021-29395 |
| globalnorthstar -- northstar_club_management | Cleartext Transmission of Sensitive Information in /northstar/Admin/login.jsp in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote local user to intercept users credentials transmitted in cleartext over HTTP. | 2022-02-04 | 5 | CVE-2021-29397 |
| globalnorthstar -- northstar_club_management | Account Hijacking in /northstar/Admin/changePassword.jsp in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote authenticated users to change the password of any targeted user accounts via lack of proper authorization in the user-controlled "userID" parameter of the HTTP POST request. | 2022-02-04 | 4 | CVE-2021-29394 |
| globalnorthstar -- northstar_club_management | Directory traversal in /northstar/Common/NorthFileManager/fileManagerObjects.jsp Northstar Technologies Inc NorthStar Club Management 6.3 allows remote unauthenticated users to browse and list the directories across the entire filesystem of the host of the web application. | 2022-02-04 | 5 | CVE-2021-29398 |
| google -- android | In fb driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges | 2022-02-09 | 4.6 | CVE-2022-20031 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | needed. User interaction is not needed for exploitation. Patch ID: ALPS05850708; Issue ID: ALPS05850708. | | | |
| google -- android | In vow driver, there is a possible out of bounds write due to a stack-based buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05837793; Issue ID: ALPS05837793. | 2022-02-09 | 4.6 | CVE-2022-20030 |
| google -- android | In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06198663; Issue ID: ALPS06198663. | 2022-02-09 | 4.6 | CVE-2022-20028 |
| google -- android | In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126832; Issue ID: ALPS06126832. | 2022-02-09 | 4.6 | CVE-2022-20025 |
| google -- android | In Preloader XFLASH, there is a possible escalation of privilege due to an improper certificate validation. This could lead to local escalation of privilege for an attacker who has physical access to the device with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06160806; Issue ID: ALPS06160806. | 2022-02-09 | 4.6 | CVE-2022-20034 |
| google -- android | In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126827; Issue ID: ALPS06126827. | 2022-02-09 | 4.6 | CVE-2022-20026 |
| google -- android | In Bluetooth, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06126826; Issue ID: ALPS06126826. | 2022-02-09 | 4.6 | CVE-2022-20027 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. The `GraphDef` format in TensorFlow does not allow self recursive functions. The runtime assumes that this invariant is satisfied. However, a `GraphDef` containing a fragment such as the following can be consumed when loading a `SavedModel`. This would result in a stack overflow during execution as resolving each `NodeDef` means resolving the function itself and its nodes. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 5 | CVE-2022-23591 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. When decoding a tensor from protobuf, TensorFlow might do a null-dereference if attributes of some mutable arguments to some operations are missing from the proto. This is guarded by a `DCHECK`. However, `DCHECK` is a no-op in production builds and an assertion failure in debug builds. In the first case execution proceeds to the dereferencing of the null pointer, whereas in the second case it results in a crash due to the assertion failure. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, and TensorFlow 2.6.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23570 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. When decoding a tensor from protobuf, a TensorFlow process can encounter cases where a `CHECK` assertion is invalidated based on user controlled arguments, if the tensors have an invalid `dtype` and 0 elements or an invalid shape. This allows attackers to cause denial of services in TensorFlow processes. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23571 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. Under certain scenarios, TensorFlow can fail to specialize a type during shape inference. This case is covered by the `DCHECK` function however, `DCHECK` is a no-op in production builds and an assertion failure in debug builds. In the first case execution proceeds to the `ValueOrDie` line. This results in an assertion failure as `ret` contains an error `Status`, not a value. In the second case we also get a crash due to the assertion failure. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, and TensorFlow 2.6.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23572 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. The implementation of `OpLevelCostEstimator::CalculateTensorSize` is vulnerable to an integer overflow if an attacker can create an operation which would involve a tensor with large enough number of elements. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23575 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. The implementation of `OpLevelCostEstimator::CalculateOutputSize` is vulnerable to an integer overflow if an attacker can create an operation which would involve tensors with large enough number of elements. We can have a large enough number of dimensions in `output_shape.dim()` or just a small number of dimensions being large enough to cause an overflow in the multiplication. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23576 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. The Grappler optimizer in TensorFlow can be used to cause a denial of service by altering a `SavedModel` such that `SafeToRemoveIdentity` would trigger `CHECK` failures. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 5 | CVE-2022-23579 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. During shape inference, TensorFlow can allocate a large vector based on a value from a tensor controlled by the user. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 5 | CVE-2022-23580 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. The Grappler optimizer in TensorFlow can be used to cause a denial of service by altering a `SavedModel` such that `IsSimplifiableReshape` would trigger `CHECK` failures. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 5 | CVE-2022-23581 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. The implementation of `GetInitOp` is vulnerable to a crash caused by dereferencing a null pointer. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23577 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. The `simplifyBroadcast` function in the MLIR-TFRT infrastructure in TensorFlow is vulnerable to a segfault (hence, denial of service), if called with scalar shapes. If all shapes are scalar, then `maxRank` is 0, so we build an empty `SmallVector`. The fix will be included in TensorFlow 2.8.0. This is the only affected version. | 2022-02-04 | 5 | CVE-2022-23593 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. When decoding a resource handle tensor from protobuf, a TensorFlow process can encounter cases | 2022-02-04 | 4 | CVE-2022-23564 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | where a `CHECK` assertion is invalidated based on user controlled arguments. This allows attackers to cause denial of services in TensorFlow processes. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | | | |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. If a graph node is invalid, TensorFlow can leak memory in the implementation of `ImmutableExecutorState::Initialize`. Here, we set `item->kernel` to `nullptr` but it is a simple `OpKernel*` pointer so the memory that was previously allocated to it would leak. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23578 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a `SavedModel` such that `TensorByteSize` would trigger `CHECK` failures. `TensorShape` constructor throws a `CHECK`-fail if shape is partial or has a number of elements that would overflow the size of an `int`. The `PartialTensorShape` constructor instead does not cause a `CHECK`-abort if the shape is partial, which is exactly what this function needs to be able to return `-1`. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23582 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a `SavedModel` such that any binary op would trigger `CHECK` failures. This occurs when the protobuf part corresponding to the tensor arguments is modified such that the `dtype` no longer matches the `dtype` expected by the op. In that case, calling the templated binary operator for the binary op would receive corrupted data, due to the type confusion involved. If `Tin` and `Tout` don't match the type of data in `out` and `input_*` tensors then `flat<*>` would interpret it wrongly. In most cases, this would be a silent failure, but we have noticed scenarios where this results in a `CHECK` crash, hence a denial of service. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23583 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a use after free behavior when decoding PNG images. After `png::CommonFreeDecode(&decode)` gets called, the values of `decode.width` and `decode.height` are in an unspecified state. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23584 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. When decoding PNG images TensorFlow can produce a memory leak if the image is invalid. After calling `png::CommonInitDecode(..., &decode)`, the `decode` value contains allocated buffers which can only be freed by calling `png::CommonFreeDecode(&decode)`. However, several error case in the function implementation invoke the `OP_REQUIRES` macro which immediately terminates the execution of the function, without allowing for the memory free to occur. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23585 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a `SavedModel` such that assertions in `function.cc` would be falsified and crash the Python interpreter. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow | 2022-02-04 | 4 | CVE-2022-23586 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | | | |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. A malicious user can cause a denial of service by altering a `SavedModel` such that Grappler optimizer would attempt to build a tensor using a reference `dtype`. This would result in a crash due to a `CHECK`-fail in the `Tensor` constructor as reference types are not allowed. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23588 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. Under certain scenarios, Grappler component of TensorFlow can trigger a null pointer dereference. There are 2 places where this can occur, for the same malicious alteration of a `SavedModel` file (fixing the first one would trigger the same dereference in the second place). First, during constant folding, the `GraphDef` might not have the required nodes for the binary operation. If a node is missing, the correposning `mul_*child` would be null, and the dereference in the subsequent line would be incorrect. We have a similar issue during `IsIdentityConsumingSwitch`. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23589 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. When building an XLA compilation cache, if default settings are used, TensorFlow triggers a null pointer dereference. In the default scenario, all devices are allowed, so `flr->config_proto` is `nullptr`. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23595 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. An attacker can trigger denial of service via assertion failure by altering a `SavedModel` on disk such that `AttrDef`s of some operation are duplicated. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23565 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. A `GraphDef` from a TensorFlow `SavedModel` can be maliciously altered to cause a TensorFlow process to crash due to encountering a `StatusOr` value that is an error and forcibly extracting the value from it. We have patched the issue in multiple GitHub commits and these will be included in TensorFlow 2.8.0 and TensorFlow 2.7.1, as both are affected. | 2022-02-04 | 5 | CVE-2022-23590 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that would cause a write outside of bounds of an array in TFLite. In fact, the attacker can override the linked list used by the memory allocator. This can be leveraged for an arbitrary write primitive under certain conditions. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 6.5 | CVE-2022-23561 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that would allow limited reads and writes outside of arrays in TFLite. This exploits missing validation in the conversion from sparse tensors to dense tensors. The fix is included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. Users are advised to upgrade as soon as possible. | 2022-02-04 | 6.5 | CVE-2022-23560 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that would trigger a division by zero in `BiasAndClamp` implementation. There is no check that the `bias_size` is non zero. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 4 | CVE-2022-23557 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. TensorFlow's type inference can cause a heap out of bounds read as the bounds checking is done in a `DCHECK` (which is a no-op during production). An attacker can control the `input_idx` variable such that `ix` would be larger than the number of values in `node_t.args`. The fix will be included in TensorFlow 2.8.0. This is the only affected version. | 2022-02-04 | 5.5 | CVE-2022-23592 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. There is a typo in TensorFlow's `SpecializeType` which results in heap OOB read/write. Due to a typo, `arg` is initialized to the `i`th mutable argument in a loop where the loop index is `j`. Hence it is possible to assign to `arg` from outside the vector of arguments. Since this is a mutable proto value, it allows both read and write to outside of bounds data. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, and TensorFlow 2.6.3, as these are also affected and still in supported range. | 2022-02-04 | 6.5 | CVE-2022-23574 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. The implementation of `AssignOp` can result in copying uninitialized data to a new tensor. This later results in undefined behavior. The implementation has a check that the left hand side of the assignment is initialized (to minimize number of allocations), but does not check that the right hand side is also initialized. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 6.5 | CVE-2022-23573 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. TensorFlow is vulnerable to a heap OOB write in `Grappler`. The `set_output` function writes to an array at the specified index. Hence, this gives a malicious user a write primitive. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 6.5 | CVE-2022-23566 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. The implementation of `Range` suffers from integer overflows. These can trigger undefined behavior or, in some scenarios, extremely large allocations. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 6.5 | CVE-2022-23562 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that would cause an integer overflow in `TfLiteIntArrayCreate`. The `TfLiteIntArrayGetSizeInBytes` returns an `int` instead of a `size_t`. An attacker can control model inputs such that `computed_size` overflows the size of `int` datatype. The fix will be included in TensorFlow 2.8.0. We will also cherrypick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range. | 2022-02-04 | 6.5 | CVE-2022-23558 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. An attacker can craft a TFLite model that would cause an integer overflow in embedding lookup operations. Both `embedding_size` and `lookup_size` are products of values provided by the user. Hence, a malicious user could trigger overflows in the multiplication. In certain scenarios, this can then result in heap OOB read/write. Users are advised to upgrade to a patched version. | 2022-02-04 | 6.5 | CVE-2022-23559 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| gpac -- gpac | A Null Pointer Dereference vulnerability exists in GPAC 1.1.0 via the xtra_box_write function in /box_code_base.c, which causes a Denial of Service. This vulnerability was fixed in commit 71f9871. | 2022-02-04 | 4.3 | CVE-2022-24249 |
| gpac -- gpac | NULL Pointer Dereference in GitHub repository gpac/gpac prior to 1.1.0. | 2022-02-04 | 4.3 | CVE-2021-4043 |
| grafana -- grafana | Grafana is an open-source platform for monitoring and observability. Affected versions are subject to a cross site request forgery vulnerability which allows attackers to elevate their privileges by mounting cross-origin attacks against authenticated high-privilege Grafana users (for example, Editors or Admins). An attacker can exploit this vulnerability for privilege escalation by tricking an authenticated user into inviting the attacker as a new user with high privileges. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue. | 2022-02-08 | 6.8 | CVE-2022-21703 |
| high_resolution_streaming_image_server_project -- high_resolution_streaming_image_server | IIPImage High Resolution Streaming Image Server prior to commit 882925b295a80ec992063deffc2a3b0d803c3195 is affected by an integer overflow in iipsrv.fcgi through malformed HTTP query parameters. | 2022-02-07 | 5 | CVE-2021-46389 |
| hpe -- agentless_management | A local unquoted search path security vulnerability has been identified in HPE Agentless Management Service for Windows version(s): Prior to 1.44.0.0, 10.96.0.0. This vulnerability could be exploited locally by a user with high privileges to execute malware that may lead to a loss of confidentiality, integrity, and availability. HPE has provided software updates to resolve the vulnerability in HPE Agentless Management Service for Windows. | 2022-02-04 | 4.6 | CVE-2021-29218 |
| hpe -- flexnetwork_5130_jg932a_firmware | A potential local buffer overflow vulnerability has been identified in HPE FlexNetwork 5130 EL Switch Series version: Prior to 5130_EI_7.10.R3507P02. HPE has made the following software update to resolve the vulnerability in HPE FlexNetwork 5130 EL Switch Series version 5130_EL_7.10.R3507P02. | 2022-02-04 | 4.6 | CVE-2021-29219 |
| hyphp -- hybbs2 | update_code in Admin.php in HYBBS2 through 2.3.2 allows arbitrary file upload via a crafted ZIP archive. | 2022-02-09 | 6.5 | CVE-2022-24676 |
| ibm -- power_system_ac922_\(8335-gtx\)_firmware | IBM OPENBMC OP920, OP930, and OP940 could allow an unauthenticated user to obtain sensitive information. IBM X-Force ID: 212047. | 2022-02-04 | 5 | CVE-2021-38960 XF |
| idreamsoft -- icms | In iCMS <=8.0.0, a directory traversal vulnerability allows an attacker to read arbitrary files. | 2022-02-04 | 5 | CVE-2021-44977 |
| ip2location -- country_blocker | The IP2Location Country Blocker WordPress plugin before 2.26.6 does not have CSRF check in the ip2location_country_blocker_save_rules AJAX action, allowing attackers to make a logged in admin block arbitrary country, or block all of them at once, preventing users from accessing the frontend. | 2022-02-07 | 4.3 | CVE-2021-25108 |
| ip2location -- country_blocker | The IP2Location Country Blocker WordPress plugin before 2.26.5 bans can be bypassed by using a specific parameter in the URL | 2022-02-07 | 6.4 | CVE-2021-25096 |
| ip2location -- country_blocker | The IP2Location Country Blocker WordPress plugin before 2.26.5 does not have authorisation and CSRF checks in the ip2location_country_blocker_save_rules AJAX action, allowing any authenticated users, such as subscriber to call it and block arbitrary country, or block all of them at once, preventing users from accessing the frontend. | 2022-02-07 | 5.5 | CVE-2021-25095 |
| itunesrpc-remastered_projec | iTunesRPC-Remastered is a Discord Rich Presence for iTunes on Windows utility. In affected versions iTunesRPC-Remastered did not properly sanitize user input used | 2022-02-04 | 6.4 | CVE-2022-23609 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| t -- itunesrpc-remastered | to remove files leading to file deletion only limited by the process permissions. Users are advised to upgrade as soon as possible. | | | |
| jenkins -- jenkins | Jenkins 2.333 and earlier, LTS 2.319.2 and earlier defines custom XStream converters that have not been updated to apply the protections for the vulnerability CVE-2021-43859 and allow unconstrained resource usage. | 2022-02-09 | 5 | CVE-2022-0538 MLIST |
| jpress -- jpress | A remote code execution (RCE) vulnerability in HelloWorldAddonController.java of jpress v4.2.0 allows attackers to execute arbitrary code via a crafted JAR package. | 2022-02-04 | 6.5 | CVE-2022-23330 |
| karma_project -- karma | Cross-site Scripting (XSS) - DOM in NPM karma prior to 6.3.14. | 2022-02-05 | 4.3 | CVE-2022-0437 |
| kicad -- kicad_eda | A stack-based buffer overflow vulnerability exists in the Gerber Viewer gerber and excellon DCodeNumber parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability. | 2022-02-04 | 6.8 | CVE-2022-23947 |
| kicad -- kicad_eda | A stack-based buffer overflow vulnerability exists in the Gerber Viewer gerber and excellon GCodeNumber parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability. | 2022-02-04 | 6.8 | CVE-2022-23946 |
| linuxfoundation -- argo-cd | Argo CD before 2.1.9 and 2.2.x before 2.2.4 allows directory traversal related to Helm charts because of an error in helmTemplate in repository.go. For example, an attacker may be able to discover credentials stored in a YAML file. | 2022-02-04 | 4 | CVE-2022-24348 |
| mahara -- mahara | In Mahara 20.10 before 20.10.4, 21.04 before 21.04.3, and 21.10 before 21.10.1, the names of folders in the Files area can be seen by a person not owning the folders. (Only folder names are affected. Neither file names nor file contents are affected.) | 2022-02-09 | 4 | CVE-2022-24694 |
| microfocus -- voltage_securemail | A potential Information leakage vulnerability has been identified in versions of Micro Focus Voltage SecureMail Mail Relay prior to 7.3.0.1. The vulnerability could be exploited to create an information leakage attack. | 2022-02-04 | 4 | CVE-2021-38130 |
| microsoft -- edge_chromium | Microsoft Edge (Chromium-based) Tampering Vulnerability. | 2022-02-07 | 5 | CVE-2022-23261 N/A |
| microsoft -- edge_chromium | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23262. | 2022-02-07 | 4.4 | CVE-2022-23263 N/A |
| microsoft -- edge_chromium | Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability. This CVE ID is unique from CVE-2022-23263. | 2022-02-07 | 6.8 | CVE-2022-23262 N/A |
| microweber -- microweber | Cross-Site Request Forgery (CSRF) in Packagist microweber/microweber prior to 1.2.11. | 2022-02-08 | 4.3 | CVE-2022-0505 |
| microweber -- microweber | Generation of Error Message Containing Sensitive Information in Packagist microweber/microweber prior to 1.2.11. | 2022-02-08 | 4 | CVE-2022-0504 |
| mirantis -- container_cloud_lens_extension | Lack of validation of URLs causes Mirantis Container Cloud Lens Extension before v3.1.1 to open external programs other than the default browser to perform sign on to a new cluster. An attacker could host a webserver which serves a malicious Mirantis Container Cloud configuration file and induce the victim to add a new cluster via its URL. This issue affects: Mirantis Mirantis Container Cloud Lens Extension v3 versions prior to v3.1.1. | 2022-02-04 | 6.8 | CVE-2022-0484 |
| mongodb -- mongodb | An authenticated user without any specific authorizations may be able to repeatedly invoke the features command where at a high volume may lead to resource depletion or generate high lock contention. This may result in denial of service and in rare cases could result in id field collisions. | 2022-02-04 | 5.5 | CVE-2021-32036 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| mruby -- mruby | Out-of-bounds Read in Homebrew mruby prior to 3.2. | 2022-02-09 | 6.4 | CVE-2022-0525 |
| msi -- app_player | Micro-Star International (MSI) App Player <= 4.280.1.6309 is vulnerable to multiple Privilege Escalation (LPE/EoP) vulnerabilities in the NTIOLib_X64.sys and BstkDrv_msi2.sys drivers components. All the vulnerabilities are triggered by sending specific IOCTL requests. | 2022-02-04 | 4.6 | CVE-2021-44900 |
| msi -- center | Micro-Star International (MSI) Center <= 1.0.31.0 is vulnerable to multiple Privilege Escalation vulnerabilities in the atidgllk.sys, atillk64.sys, MODAPI.sys, NTIOLib.sys, NTIOLib_X64.sys, WinRing0.sys, WinRing0x64.sys drivers components. All the vulnerabilities are triggered by sending specific IOCTL requests. | 2022-02-04 | 4.6 | CVE-2021-44899 |
| msi -- center_pro | Micro-Star International (MSI) Center Pro <= 2.0.16.0 is vulnerable to multiple Privilege Escalation (LPE/EoP) vulnerabilities in the atidgllk.sys, atillk64.sys, MODAPI.sys, NTIOLib.sys, NTIOLib_X64.sys, WinRing0.sys, WinRing0x64.sys drivers components. All the vulnerabilities are triggered by sending specific IOCTL requests. | 2022-02-04 | 4.6 | CVE-2021-44903 |
| msi -- dragon_center | Micro-Star International (MSI) Dragon Center <= 2.0.116.0 is vulnerable to multiple Privilege Escalation (LPE/EoP) vulnerabilities in the atidgllk.sys, atillk64.sys, MODAPI.sys, NTIOLib.sys, NTIOLib_X64.sys, WinRing0.sys, WinRing0x64.sys drivers components. All the vulnerabilities are triggered by sending specific IOCTL requests. | 2022-02-04 | 4.6 | CVE-2021-44901 |
| nvidia -- gpu_display_driver | NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for private IOCTLs where a NULL pointer dereference in the kernel, created within user mode code, may lead to a denial of service in the form of a system crash. | 2022-02-07 | 4.9 | CVE-2022-21815 |
| nvidia -- virtual_gpu | NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager (nvidia.ko), where a user in the guest OS can cause a GPU interrupt storm on the hypervisor host, leading to a denial of service. | 2022-02-07 | 4.9 | CVE-2022-21816 |
| ocproducts -- composr | Authenticated remote code execution (RCE) in Composr-CMS 10.0.39 and earlier allows remote attackers to execute arbitrary code via uploading a PHP shell through /adminzone/index.php?page=admin-commandr. | 2022-02-09 | 6.5 | CVE-2021-46360 |
| octopus -- octopus_deploy | In affected Octopus Server versions when the server HTTP and HTTPS bindings are configured to localhost, Octopus Server will allow open redirects. | 2022-02-07 | 5.8 | CVE-2022-23184 |
| openzeppelin -- openzeppelin | In OpenZeppelin <=v4.4.0, initializer functions that are invoked separate from contract creation (the most prominent example being minimal proxies) may be reentered if they make an untrusted non-view external call. Once an initializer has finished running it can never be re-executed. However, an exception put in place to support multiple inheritance made reentrancy possible, breaking the expectation that there is a single execution. | 2022-02-04 | 5 | CVE-2021-46320 |
| publify_project -- publify | Business Logic Errors in GitHub repository publify/publify prior to 9.2.7. | 2022-02-08 | 5 | CVE-2022-0524 |
| quickbox -- quickbox | QuickBox Pro v2.4.8 contains a cross-site scripting (XSS) vulnerability at "adminuseredit.php?usertoedit=XSS", as the user supplied input for the value of this parameter is not properly sanitized. | 2022-02-07 | 4.3 | CVE-2021-45281 |
| radare -- radare2 | Expired Pointer Dereference in GitHub repository radareorg/radare2 prior to 5.6.2. | 2022-02-08 | 6.8 | CVE-2022-0523 |
| radare -- radare2 | Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.6.2. | 2022-02-08 | 5.8 | CVE-2022-0518 |
| radare -- radare2 | Buffer Access with Incorrect Length Value in GitHub repository radareorg/radare2 prior to 5.6.2. | 2022-02-08 | 5.8 | CVE-2022-0519 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| radare -- radare2 | Access of Memory Location After End of Buffer in GitHub repository radareorg/radare2 prior to 5.6.2. | 2022-02-08 | 5.8 | CVE-2022-0521 |
| radare -- radare2 | Use After Free in NPM radare2.js prior to 5.6.2. | 2022-02-08 | 6.8 | CVE-2022-0520 |
| radare -- radare2 | Access of Memory Location Before Start of Buffer in NPM radare2.js prior to 5.6.2. | 2022-02-08 | 5.8 | CVE-2022-0522 |
| rearrange_woocommerce_products_project -- rearrange_woocommerce_products | The Rearrange Woocommerce Products WordPress plugin before 3.0.8 does not have proper access controls in the save_all_order AJAX action, nor validation and escaping when inserting user data in SQL statement, leading to an SQL injection, and allowing any authenticated user, such as subscriber, to modify arbitrary post content (for example with an XSS payload), as well as exfiltrate any data by copying it to another post. | 2022-02-07 | 4 | CVE-2021-24928 |
| sap -- netweaver_application_server_java | Due to improper error handling in SAP NetWeaver Application Server Java - versions KRNL64NUC 7.22, 7.22EXT, 7.49, KRNL64UC, 7.22, 7.22EXT, 7.49, 7.53, KERNEL 7.22, 7.49, 7.53, an attacker could submit multiple HTTP server requests resulting in errors, such that it consumes the memory buffer. This could result in system shutdown rendering the system unavailable. | 2022-02-09 | 5 | CVE-2022-22533 |
| schneider-electric -- bmxp342020_firmware | A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists on the web server used, that could cause a leak of sensitive data or unauthorized actions on the web server during the time the user is logged in. Affected Products: Modicon M340 CPUs: BMXP34 (All Versions), Modicon Quantum CPUs with integrated Ethernet (Copro): 140CPU65 (All Versions), Modicon Premium CPUs with integrated Ethernet (Copro): TSXP57 (All Versions), Modicon M340 ethernet modules: (BMXNOC0401, BMXNOE01, BMXNOR0200H) (All Versions), Modicon Quantum and Premium factory cast communication modules: (140NOE77111, 140NOC78*00, TSXETY5103, TSXETY4103) (All Versions) | 2022-02-04 | 6.8 | CVE-2020-7534 |
| schneider-electric -- easergy_p5_firmware | A CWE-798: Use of Hard-coded Credentials vulnerability exists that could result in information disclosure. If an attacker were to obtain the SSH cryptographic key for the device and take active control of the local operational network connected to the product they could potentially observe and manipulate traffic associated with product configuration. Affected Product: Easergy P5 (All firmware versions prior to V01.401.101) | 2022-02-04 | 5.4 | CVE-2022-22722 |
| schneider-electric -- ecostruxure_power_monitoring_expert | A CWE-20: Improper Input Validation vulnerability exists that could allow arbitrary files on the server to be read by authenticated users through a limited operating system service account. Affected Product: EcoStruxure Power Monitoring Expert (Versions 2020 and prior) | 2022-02-04 | 4 | CVE-2022-22726 |
| sealevel -- seaconnect_370w_firmware | An out-of-bounds write vulnerability exists in the URL_decode functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A specially-crafted MQTT payload can lead to an out-of-bounds write. An attacker can perform a man-in-the-middle attack to trigger this vulnerability. | 2022-02-04 | 4.3 | CVE-2021-21971 |
| sealevel -- seaconnect_370w_firmware | An out-of-bounds write vulnerability exists in the HandleSeaCloudMessage functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. The HandleIncomingSeaCloudMessage function uses at [4] the json_object_get_string to populate the p_payload global variable. The p_payload is only 0x100 bytes long, and the total MQTT message could be up to 0x201 bytes. Because the function json_object_get_string will fill str based on the length of the json's value and not the actual str size, this would result in a possible out-of-bounds write. | 2022-02-04 | 6.8 | CVE-2021-21969 |
| sealevel -- seaconnect_370w_firmware | An information disclosure vulnerability exists in the Web Server functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A specially-crafted man-in-the-middle attack can lead to a disclosure of sensitive information. An attacker can perform a man-in-the-middle attack to trigger this vulnerability. | 2022-02-04 | 4.3 | CVE-2021-21963 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| sealevel -- seaconnect_370w_firmware | A onfiguration exists in the MQTTS functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. This onfiguration significantly simplifies a man-in-the-middle attack, which directly leads to control of device functionality. | 2022-02-04 | 6.8 | CVE-2021-21959 |
| sealevel -- seaconnect_370w_firmware | A denial of service vulnerability exists in the SeaMax remote configuration functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. Specially-crafted network packets can lead to denial of service. An attacker can send a malicious packet to trigger this vulnerability. | 2022-02-04 | 6.4 | CVE-2021-21965 |
| sealevel -- seaconnect_370w_firmware | A file write vulnerability exists in the OTA update task functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A specially-crafted MQTT payload can lead to arbitrary file overwrite. An attacker can perform a man-in-the-middle attack to trigger this vulnerability. | 2022-02-04 | 5.8 | CVE-2021-21968 |
| sealevel -- seaconnect_370w_firmware | An out-of-bounds write vulnerability exists in the HandleSeaCloudMessage functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. The HandleIncomingSeaCloudMessage function uses at [3] the json_object_get_string to populate the p_name global variable. The p_name is only 0x80 bytes long, and the total MQTT message could be up to 0x201 bytes. Because the function json_object_get_string will fill str based on the length of the json's value and not the actual str size, this would result in a possible out-of-bounds write. | 2022-02-04 | 6.8 | CVE-2021-21970 |
| sealevel -- seaconnect_370w_firmware | A heap-based buffer overflow vulnerability exists in the OTA Update u-download functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. A series of specially-crafted MQTT payloads can lead to remote code execution. An attacker must perform a man-in-the-middle attack in order to trigger this vulnerability. | 2022-02-04 | 6.8 | CVE-2021-21962 |
| seeddms -- seeddms | Open Redirect vulnerability exists in SeedDMS 6.0.15 in out.Login.php, which llows remote malicious users to redirect users to malicious sites using the "referuri" parameter. | 2022-02-04 | 5.8 | CVE-2021-45408 |
| servisnet -- tessa | An issue was discovered in Servisnet Tessa 0.0.2. An attacker can obtain sensitive information via a /js/app.js request. | 2022-02-06 | 5 | CVE-2022-22833 |
| seur_oficial_project -- seur_oficial | The SEUR Oficial WordPress plugin before 1.7.2 creates a PHP file with a random name when installed, even though it is used for support purposes, it allows to download any file from the web server without restriction after knowing the URL and a password than an administrator can see in the plugin settings page. | 2022-02-07 | 4 | CVE-2021-25004 |
| shibboleth -- oidc_op | The OIDC OP plugin before 3.0.4 for Shibboleth Identity Provider allows server-side request forgery (SSRF) due to insufficient restriction of the request_uri parameter. This allows attackers to interact with arbitrary third-party HTTP services. | 2022-02-04 | 6.4 | CVE-2022-24129 |
| siemens -- simcenter_femap | A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a stack based buffer overflow vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14683, ZDI-CAN-15283, ZDI-CAN-15303, ZDI-CAN-15593) | 2022-02-09 | 6.8 | CVE-2021-46155 |
| siemens -- simcenter_femap | A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a stack based buffer overflow vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15085, ZDI-CAN-15289, ZDI-CAN-15602) | 2022-02-09 | 6.8 | CVE-2021-46158 |
| siemens -- simcenter_femap | A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15050) | 2022-02-09 | 6.8 | CVE-2021-46159 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| siemens -- simcenter_femap | A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15286) | 2022-02-09 | 6.8 | CVE-2021-46160 |
| siemens -- simcenter_femap | A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14684) | 2022-02-09 | 6.8 | CVE-2021-46156 |
| siemens -- simcenter_femap | A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15302) | 2022-02-09 | 6.8 | CVE-2021-46161 |
| siemens -- simcenter_femap | A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a stack based buffer overflow vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14646, ZDI-CAN-14679, ZDI-CAN-15084, ZDI-CAN-15304) | 2022-02-09 | 6.8 | CVE-2021-46154 |
| siemens -- simcenter_femap | A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a memory corruption vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14757) | 2022-02-09 | 6.8 | CVE-2021-46157 |
| siemens -- simcenter_femap | A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a memory corruption vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14645, ZDI-CAN-15305, ZDI-CAN-15589, ZDI-CAN-15599) | 2022-02-09 | 6.8 | CVE-2021-46153 |
| siemens -- simcenter_femap | A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains a type confusion vulnerability while parsing NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14643, ZDI-CAN-14644, ZDI-CAN-14755, ZDI-CAN-15183) | 2022-02-09 | 6.8 | CVE-2021-46152 |
| siemens -- simcenter_femap | A vulnerability has been identified in Simcenter Femap V2020.2 (All versions), Simcenter Femap V2021.1 (All versions). Affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-14754, ZDI-CAN-15082) | 2022-02-09 | 6.8 | CVE-2021-46151 |
| silabs -- zgm130s037hgn_firmware | The Z-Wave specification requires that S2 security can be downgraded to S0 or other less secure protocols, allowing an attacker within radio range during pairing to downgrade and then exploit a different vulnerability (CVE-2013-20003) to intercept and spoof traffic. | 2022-02-04 | 4.8 | CVE-2018-25029 |
| silverstripe -- silverstripe | Business Logic Errors in GitHub repository silverstripe/silverstripe-framework prior to 4.10.1. | 2022-02-04 | 4 | CVE-2022-0227 |
| starwindsoftware -- iscsi_san | StarWind iSCSI SAN before 3.5 build 2007-08-09 allows socket exhaustion. | 2022-02-06 | 5 | CVE-2007-20001 |
| supportcandy -- supportcandy | The SupportCandy WordPress plugin before 2.2.7 does not sanitise and escape the query string before outputting it back in pages with the [wpsc_create_ticket] shortcode embed, leading to a Reflected Cross-Site Scripting issue | 2022-02-07 | 4.3 | CVE-2021-24878 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| supportcandy -- supportcandy | The SupportCandy WordPress plugin before 2.2.7 does not have CRSF check in its wpsc_tickets AJAX action, which could allow attackers to make a logged in admin call it and delete arbitrary tickets via the set_delete_permanently_bulk_ticket setting_action. | 2022-02-07 | 4.3 | CVE-2021-24843 |
| supportcandy -- supportcandy | The SupportCandy WordPress plugin before 2.2.7 does not have CSRF check in the wpsc_tickets AJAX action, nor has any sanitisation or escaping in some of the filter fields which could allow attackers to make a logged in user having access to the ticket lists dashboard set an arbitrary filter (stored in their cookies) with an XSS payload in it. | 2022-02-07 | 6.8 | CVE-2021-24879 |
| supportcandy -- supportcandy | The SupportCandy WordPress plugin before 2.2.5 does not have authorisation and CSRF checks in its wpsc_tickets AJAX action, which could allow unauthenticated users to call it and delete arbitrary tickets via the set_delete_permanently_bulk_ticket setting_action. Other actions may be affected as well. | 2022-02-07 | 4.3 | CVE-2021-24839 |
| synology -- diskstation_manager | Exposure of sensitive information to an unauthorized actor vulnerability in Web Server in Synology DiskStation Manager (DSM) before 7.0.1-42218-2 allows remote attackers to obtain sensitive information via unspecified vectors. | 2022-02-07 | 5 | CVE-2022-22680 |
| synology -- diskstation_manager | Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in support service management in Synology DiskStation Manager (DSM) before 7.0.1-42218-2 allows remote authenticated users to write arbitrary files via unspecified vectors. | 2022-02-07 | 4 | CVE-2022-22679 |
| synology -- diskstation_manager | Improper neutralization of special elements in output used by a downstream component ('Injection') vulnerability in work flow management in Synology DiskStation Manager (DSM) before 7.0.1-42218-2 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. | 2022-02-07 | 4 | CVE-2021-43929 |
| synology -- mail_station | Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in mail sending and receiving component in Synology Mail Station before 7.0.1-42218-2 allows remote authenticated users to execute arbitrary commands via unspecified vectors. | 2022-02-07 | 6.5 | CVE-2021-43928 |
| taogogo -- taocms | An issue was discovered in taoCMS v3.0.2. There is an arbitrary file read vulnerability that can read any files via admin.php?action=file&ctrl=download&path=../../1.txt. | 2022-02-04 | 4 | CVE-2022-23316 |
| taogogo -- taocms | In taocms 3.0.1 after logging in to the background, there is an Arbitrary file download vulnerability at the File Management column. | 2022-02-04 | 4 | CVE-2021-44983 |
| thinkupthemes -- responsive_vector_maps | The RVM WordPress plugin before 6.4.2 does not have proper authorisation, CSRF checks and validation of the rvm_upload_regions_file_path parameter in the rvm_import_regions AJAX action, allowing any authenticated user, such as subscriber, to read arbitrary files on the web server | 2022-02-07 | 4 | CVE-2021-24947 |
| tp-link -- wn886n_firmware | TP-Link WR886N 3.0 1.0.1 Build 150127 Rel.34123n is vulnerable to Buffer Overflow. Authenticated attackers can crash router httpd services via /userRpm/PingIframeRpm.htm request which contains redundant & in parameter. | 2022-02-08 | 4 | CVE-2021-44864 |
| twistedmatrix -- twisted | twisted is an event-driven networking engine written in Python. In affected versions twisted exposes cookies and authorization headers when following cross-origin redirects. This issue is present in the `twited.web.RedirectAgent` and `twisted.web. BrowserLikeRedirectAgent` functions. Users are advised to upgrade. There are no known workarounds. | 2022-02-07 | 5 | CVE-2022-21712 |
| virustotal -- yara | A Buffer Overflow vulnerablity exists in VirusTotal YARA git commit: 605b2edf07ed8eb9a2c61ba22eb2e7c362f47ba7 via yr_set_configuration in yara/libyara/libyara.c, which could cause a Denial of Service. | 2022-02-04 | 4.3 | CVE-2021-45429 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| visser -- store_exporter_for_woocommerce | The WooCommerce Stored Exporter WordPress plugin before 2.7.1 was affected by a Reflected Cross-Site Scripting (XSS) vulnerability in the woo_ce admin page. | 2022-02-07 | 4.3 | CVE-2022-0149 |
| visser -- store_toolkit_for_woocommerce | The Store Toolkit for WooCommerce WordPress plugin before 2.3.2 does not sanitise and escape the tab parameter before outputting it back in an admin page in an error message, leading to a Reflected Cross-Site Scripting | 2022-02-07 | 4.3 | CVE-2021-25077 |
| vmware -- cloud_foundation | VMware Cloud Foundation contains an information disclosure vulnerability due to logging of credentials in plain-text within multiple log files on the SDDC Manager. A malicious actor with root access on VMware Cloud Foundation SDDC Manager may be able to view credentials in plaintext within one or more log files. | 2022-02-04 | 4 | CVE-2022-22939 |
| voipmonitor -- voipmonitor | The config restore function of Voipmonitor GUI before v24.96 does not properly check files sent as restore archives, allowing remote attackers to execute arbitrary commands via a crafted file in the web root. | 2022-02-04 | 6.8 | CVE-2022-24262 |
| xwiki -- xwiki | ### Impact It's possible to know if a user has or not an account in a wiki related to an email address, and which username(s) is actually tied to that email by forging a request to the Forgot username page. Note that since this page does not have a CSRF check it's quite easy to perform a lot of those requests. ### Patches This issue has been patched in XWiki 12.10.5 and 13.2RC1. Two different patches are provided: - a first one to fix the CSRF problem - a more complex one that now relies on sending an email for the Forgot username process. ### Workarounds It's possible to fix the problem without uprading by editing the ForgotUsername page in version below 13.x, to use the following code: https://github.com/xwiki/xwiki-platform/blob/69548c0320cbd772540cf4668743e69f879812cf/xwiki-platform-core/xwiki-platform-administration/xwiki-platform-administration-ui/src/main/resources/XWiki/ForgotUsername.xml#L39-L123 In version after 13.x it's also possible to edit manually the forgotusername.vm file, but it's really encouraged to upgrade the version here. ### References * https://jira.xwiki.org/browse/XWIKI-18384 * https://jira.xwiki.org/browse/XWIKI-18408 ### For more information If you have any questions or comments about this advisory: * Open an issue in [Jira XWiki](https://jira.xwiki.org) * Email us at [security ML](mailto:security@xwiki.org) | 2022-02-04 | 4.3 | CVE-2021-32732 |
| yet_another_stars_rating_project -- yet_another_stars_rating | Cross-Site Scripting (XSS) vulnerability discovered in Yasr – Yet Another Stars Rating WordPress plugin (versions <= 2.9.9), vulnerable at parameter 'source'. | 2022-02-04 | 4.3 | CVE-2022-23980 |
| zammad -- zammad | In Zammad 5.0.2, agents can configure "out of office" periods and substitute persons. If the substitute persons didn't have the same permissions as the original agent, they could receive ticket notifications for tickets that they have no access to. | 2022-02-04 | 5 | CVE-2021-44886 |
| zammad -- zammad | With certain LDAP configurations, Zammad 5.0.1 was found to be vulnerable to unauthorized access with existing user accounts. | 2022-02-04 | 5.5 | CVE-2021-43145 |
| zephyrproject -- zephyr | Buffer overflow in usb device class. Zephyr versions >= v2.6.0 contain Heap-based Buffer Overflow (CWE-122). For more information, see https://github.com/zephyrproject-rtos/zephyr/security/advisories/GHSA-fm6v-8625-99jf | 2022-02-07 | 5.8 | CVE-2021-3835 N/A |
| zimbra -- collaboration | An issue was discovered in the Calendar feature in Zimbra Collaboration Suite 8.8.x before 8.8.15 patch 30 (update 1), as exploited in the wild starting in December 2021. An attacker could place HTML containing executable JavaScript inside element attributes. This markup becomes unescaped, causing arbitrary markup to be injected into the document. | 2022-02-09 | 4.3 | CVE-2022-24682 |
| 10web -- spidercalendar | The SpiderCalendar WordPress plugin through 1.5.65 does not sanitise and escape the callback parameter before outputting it back in the page via the window AJAX | 2022-02-14 | 4.3 | CVE-2022-0212 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | action (available to both unauthenticated and authenticated users), leading to a Reflected Cross-Site Scripting issue. | | | |
| apache -- cayenne | Hessian serialization is a network protocol that supports object-based transmission. Apache Cayenne's optional Remote Object Persistence (ROP) feature is a web services-based technology that provides object persistence and query functionality to 'remote' applications. In Apache Cayenne 4.1 and earlier, running on non-current patch versions of Java, an attacker with client access to Cayenne ROP can transmit a malicious payload to any vulnerable third-party dependency on the server. This can result in arbitrary code execution. | 2022-02-11 | 6.5 | CVE-2022-24289<br>MLIST |
| appneta -- tcpreplay | tcpreplay 4.3.4 has a Reachable Assertion in add_tree_ipv4() at tree.c. | 2022-02-11 | 4.3 | CVE-2021-45387 |
| appneta -- tcpreplay | tcpreplay 4.3.4 has a Reachable Assertion in add_tree_ipv6() at tree.c | 2022-02-11 | 4.3 | CVE-2021-45386 |
| drupal -- drupal | The QuickEdit module does not properly check access to fields in some circumstances, which can lead to unintended disclosure of field data. Sites are only affected if the QuickEdit module (which comes with the Standard profile) is installed. | 2022-02-11 | 4 | CVE-2020-13676 |
| drupal -- drupal | Under some circumstances, the Drupal core JSON:API module does not properly restrict access to certain content, which may result in unintended access bypass. Sites that do not have the JSON:API module enabled are not affected. | 2022-02-11 | 4.3 | CVE-2020-13677 |
| drupal -- drupal | The QuickEdit module does not properly validate access to routes, which could allow cross-site request forgery under some circumstances and lead to possible data integrity issues. Sites are only affected if the QuickEdit module (which comes with the Standard profile) is installed. Removing the "access in-place editing" permission from untrusted users will not fully mitigate the vulnerability. | 2022-02-11 | 4.3 | CVE-2020-13674 |
| drupal -- drupal | Cross-site Scripting (XSS) vulnerability in ckeditor of Drupal Core allows attacker to inject XSS. This issue affects: Drupal Core 8.8.x versions prior to 8.8.10.; 8.9.x versions prior to 8.9.6; 9.0.x versions prior to 9.0.6. | 2022-02-11 | 4.3 | CVE-2020-13669 |
| fastify -- fastify-multipart | This affects the package fastify-multipart before 5.3.1. By providing a name=constructor property it is still possible to crash the application. **Note:** This is a bypass of CVE-2020-8136 (https://security.snyk.io/vuln/SNYK-JS-FASTIFYMULTIPART-1290382). | 2022-02-11 | 5 | CVE-2021-23597 |
| ffjpeg_project -- ffjpeg | A Null Pointer Dereference vulnerability exits in ffjpeg d5cfd49 (2021-12-06) in bmp_load(). When the size information in metadata of the bmp is out of range, it returns without assign memory buffer to `pb->pdata` and did not exit the program. So the program crashes when it tries to access the pb->data, in jfif_encode() at jfif.c:763. This is due to the incomplete patch for CVE-2020-13438. | 2022-02-11 | 4.3 | CVE-2021-45385 |
| golang -- go | Curve.IsOnCurve in crypto/elliptic in Go before 1.16.14 and 1.17.x before 1.17.7 can incorrectly return true in situations with a big.Int value that is not a valid field element. | 2022-02-11 | 6.4 | CVE-2022-23806 |
| golang -- go | cmd/go in Go before 1.16.14 and 1.17.x before 1.17.7 can misinterpret branch names that falsely appear to be version tags. This can lead to incorrect access control if an actor is supposed to be able to create branches but not tags. | 2022-02-11 | 5 | CVE-2022-23773 |
| google -- android | Unprotected dynamic receiver in Telecom prior to SMR Feb-2022 Release 1 allows untrusted applications to launch arbitrary activity. | 2022-02-11 | 4.6 | CVE-2022-22292 |
| google -- android | In startVideoStream() there is a possibility of an OOB Read in the heap, when the camera buffer is ‘zero’ in size.Product: AndroidVersions: Android-11Android ID: A-205097028 | 2022-02-11 | 5 | CVE-2021-39677 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- android | In onCreate of InstallCaCertificateWarning.java, there is a possible way to mislead an user about CA installation circumstances due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-196969991 | 2022-02-11 | 4.4 | CVE-2021-39669 |
| google -- android | An improper boundary check in RPMB ldfw prior to SMR Feb-2022 Release 1 allows arbitrary memory write and code execution. | 2022-02-11 | 4.6 | CVE-2022-23431 |
| google -- android | An improper input validation in SMC_SRPMB_WSM handler of RPMB ldfw prior to SMR Feb-2022 Release 1 allows arbitrary memory write and code execution. | 2022-02-11 | 4.6 | CVE-2022-23432 |
| google -- android | In checkSpsUpdated of AAVCAssembler.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-204077881 | 2022-02-11 | 4.3 | CVE-2021-39665 |
| google -- android | In code generated by aidl_const_expressions.cpp, there is a possible out of bounds read due to uninitialized data. This could lead to information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-206718630 | 2022-02-11 | 4.3 | CVE-2021-39671 |
| google -- chrome | Use after free in Data Transfer in Google Chrome on Chrome OS prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0308 |
| google -- chrome | Object lifecycle issue in ANGLE in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-11 | 6.8 | CVE-2021-4100 |
| google -- chrome | Insufficient data validation in Mojo in Google Chrome prior to 96.0.4664.110 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. | 2022-02-11 | 4.3 | CVE-2021-4098 |
| google -- chrome | Inappropriate implementation in Navigation in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to incorrectly set origin via a crafted HTML page. | 2022-02-12 | 4.3 | CVE-2022-0111 |
| google -- chrome | Inappropriate implementation in Navigation in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to leak cross-origin data via a crafted HTML page. | 2022-02-12 | 4.3 | CVE-2022-0108 |
| google -- chrome | Inappropriate implementation in Autofill in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to obtain potentially sensitive information via a crafted HTML page. | 2022-02-12 | 4.3 | CVE-2022-0109 |
| google -- chrome | Use after free in Swiftshader in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-11 | 6.8 | CVE-2021-4099 |
| google -- chrome | Incorrect security UI in Autofill in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. | 2022-02-12 | 4.3 | CVE-2022-0110 |
| google -- chrome | Use after free in Optimization Guide in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0307 |
| google -- chrome | Inappropriate implementation in DevTools in Google Chrome prior to 97.0.4692.71 allowed an attacker who convinced a user to install a malicious extension to to potentially allow extension to escape the sandbox via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0097 |
| google -- chrome | Use after free in PDF Accessibility in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0105 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- chrome | Use after free in Autofill in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who convinced a user to perform specific user gesture to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0106 |
| google -- chrome | Use after free in File Manager API in Google Chrome on Chrome OS prior to 97.0.4692.71 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0107 |
| google -- chrome | Use after free in Safe browsing in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0289 |
| google -- chrome | Type confusion in V8 in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0102 |
| google -- chrome | Heap buffer overflow in Bookmarks in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who convinced a user to perform specific user gesture to potentially exploit heap corruption via specific user gesture. | 2022-02-12 | 6.8 | CVE-2022-0101 |
| google -- chrome | Use after free in Bookmarks in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0304 |
| google -- chrome | Heap buffer overflow in Media streams API in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0100 |
| google -- chrome | Use after free in Sign-in in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who convinced a user to perform specific user gestures to potentially exploit heap corruption via specific user gesture. | 2022-02-12 | 6.8 | CVE-2022-0099 |
| google -- chrome | Use after free in Screen Capture in Google Chrome on Chrome OS prior to 97.0.4692.71 allowed an attacker who convinced a user to perform specific user gestures to potentially exploit heap corruption via specific user gestures. | 2022-02-12 | 6.8 | CVE-2022-0098 |
| google -- chrome | Use after free in Site isolation in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0290 |
| google -- chrome | Use after free in Web packaging in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0293 |
| google -- chrome | Use after free in SwiftShader in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0103 |
| google -- chrome | Use after free in Storage in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0096 |
| google -- chrome | Use after free in Omnibox in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced the user to engage is specific user interactions to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0295 |
| google -- chrome | Use after free in Printing in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced the user to engage is specific user interactions to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0296 |
| google -- chrome | Use after free in V8 in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-11 | 6.8 | CVE-2021-4102 |
| google -- chrome | Use after free in Vulkan in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0297 |
| google -- chrome | Use after free in Scheduling in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0298 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- chrome | Heap buffer overflow in Swiftshader in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-11 | 6.8 | CVE-2021-4101 |
| google -- chrome | Use after free in Text Input Method Editor in Google Chrome on Android prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0300 |
| google -- chrome | Use after free in Omnibox in Google Chrome prior to 97.0.4692.99 allowed an attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0302 |
| google -- chrome | Heap buffer overflow in ANGLE in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. | 2022-02-12 | 6.8 | CVE-2022-0104 |
| kde -- kate | The LSP (Language Server Protocol) plugin in KDE Kate before 21.12.2 and KTextEditor before 5.91.0 tries to execute the associated LSP server binary when opening a file of a given type. If this binary is absent from the PATH, it will try running the LSP server binary in the directory of the file that was just opened (due to a misunderstanding of the QProcess API, that was never intended). This can be an untrusted directory. | 2022-02-11 | 6.8 | CVE-2022-23853 |
| libtiff -- libtiff | Null source pointer passed as an argument to memcpy() function within TIFFFetchStripThing() in tif_dirread.c in libtiff versions from 3.9.0 to 4.3.0 could lead to Denial of Service via crafted TIFF file. For users that compile libtiff from sources, the fix is available with commit eecb0712. | 2022-02-11 | 4.3 | CVE-2022-0561 |
| libtiff -- libtiff | Null source pointer passed as an argument to memcpy() function within TIFFReadDirectory() in tif_dirread.c in libtiff versions from 4.0 to 4.3.0 could lead to Denial of Service via crafted TIFF file. For users that compile libtiff from sources, a fix is available with commit 561599c. | 2022-02-11 | 4.3 | CVE-2022-0562 |
| linux -- linux_kernel | drivers/usb/gadget/legacy/inode.c in the Linux kernel through 5.16.8 mishandles dev->buf release. | 2022-02-11 | 4.6 | CVE-2022-24958 |
| microweber -- microweber | Open Redirect in Packagist microweber/microweber prior to 1.2.11. | 2022-02-11 | 5.8 | CVE-2022-0560 |
| permalink_manager_lite_project -- permalink_manager_lite | The Permalink Manager Lite WordPress plugin before 2.2.15 and Permalink Manager Pro WordPress plugin before 2.2.15 do not sanitise and escape query parameters before outputting them back in the debug page, leading to a Reflected Cross-Site Scripting issue | 2022-02-14 | 4.3 | CVE-2022-0201 |
| qualcomm -- apq8009w_firmware | Improper validation of input when provisioning the HDCP key can lead to memory corruption in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wearables | 2022-02-11 | 4.6 | CVE-2021-30318 |
| qualcomm -- apq8096au_firmware | Possible out of bound access of DCI resources due to lack of validation process and resource allocation in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking | 2022-02-11 | 4.6 | CVE-2021-30325 |
| qualcomm -- apq8096au_firmware | Possible out of bound write due to lack of boundary check for the maximum size of buffer when sending a DCI packet to remote process in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking | 2022-02-11 | 4.6 | CVE-2021-30324 |
| qualcomm -- ar8035_firmware | Possible assertion due to improper size validation while processing the DownlinkPreemption IE in an RRC Reconfiguration/RRC Setup message in | 2022-02-11 | 5 | CVE-2021-30326 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile | | | |
| qualcomm -- mdm9650_firmware | Improper size validation of QXDM commands can lead to memory corruption in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile | 2022-02-11 | 4.6 | CVE-2021-30309 |
| samsung -- bixby_vision | Exposure of Sensitive Information vulnerability in Bixby Vision prior to version 3.7.50.6 allows attackers to access internal data of Bixby Vision via unprotected intent. | 2022-02-11 | 5 | CVE-2022-24003 |
| samsung -- link_sharing | Improper Authorization vulnerability in Link Sharing prior to version 12.4.00.3 allows attackers to open protected activity via PreconditionActivity. | 2022-02-11 | 5 | CVE-2022-24002 |
| samsung -- reminder | Improper access control vulnerability in Reminder prior to versions 12.3.01.3000 in Android S(12), 12.2.05.6000 in Android R(11) and 11.6.08.6000 in Andoid Q(10) allows attackers to register reminders or execute exporeted activities remotely. | 2022-02-11 | 5 | CVE-2022-23433 |
| samsung -- wear_os | Unprotected component vulnerability in StTheaterModeDurationAlarmReceiver in Wear OS 3.0 prior to Firmware update Feb-2022 Release allows untrusted applications to disable theater mode without a proper permission. | 2022-02-11 | 4.3 | CVE-2022-23997 |
| schneider-electric -- interactive_graphical_scada_system_data_collector | A CWE-120: Buffer Copy without Checking Size of Input vulnerability exists that could result in denial of service, due to missing length check on user-supplied data from a constructed message received on the network. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21320 and prior) | 2022-02-11 | 5 | CVE-2021-22824 |
| schneider-electric -- interactive_graphical_scada_system_data_collector | A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause deletion of arbitrary files in the context of the user running IGSS due to lack of validation of network messages. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21320 and prior) | 2022-02-11 | 5 | CVE-2021-22823 |
| schneider-electric -- interactive_graphical_scada_system_data_collector | A CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause deletion of arbitrary files in the context of the user running IGSS due to lack of validation of network messages. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21243 and prior) | 2022-02-11 | 5 | CVE-2021-22805 |
| schneider-electric -- interactive_graphical_scada_system_data_collector | A CWE-22: Improper Limitation of a Pathname to a Restricted Directory vulnerability exists that could cause disclosure of arbitrary files being read in the context of the user running IGSS, due to missing validation of user supplied data in network messages. Affected Product: Interactive Graphical SCADA System Data Collector (dc.exe) (V15.0.0.21243 and prior) | 2022-02-11 | 5 | CVE-2021-22804 |
| schneider-electric -- modicon_m218_firmware | A CWE-20: Improper Input Validation vulnerability exists that could cause a Denial of Service when a crafted packet is sent to the controller over network port 1105/TCP. Affected Product: Modicon M218 Logic Controller (V5.1.0.6 and prior) | 2022-02-11 | 5 | CVE-2021-22800 |
| updraftplus -- updraftplus | The UpdraftPlus WordPress plugin Free before 1.22.3 and Premium before 2.22.3 do not properly validate a user has the required privileges to access a backup's nonce identifier, which may allow any users with an account on the site (such as subscriber) to download the most recent site & database backup. | 2022-02-17 | 4 | CVE-2022-0633 |
| wpbeaveraddons -- powerpack_lite_for_beaver_builder | The PowerPack Lite for Beaver Builder WordPress plugin before 1.2.9.3 does not sanitise and escape the tab parameter before outputting it back in an admin page, leading to a Reflected Cross-Site Scripting | 2022-02-14 | 4.3 | CVE-2022-0176 |

# Medium Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| wpchill -- remove_footer_credit | The Remove Footer Credit WordPress plugin before 1.0.6 does not have CSRF check in place when saving its settings, which could allow attacker to make logged in admins change them and lead to Stored XSS issue as well due to the lack of sanitisation | 2022-02-14 | 6 | CVE-2021-24446 |
| yzmcms -- yzmcms | YzmCMS v6.3 is affected by Cross Site Request Forgery (CSRF) in /admin.add | 2022-02-15 | 6.8 | CVE-2022-23384 |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| amd -- epyc_7763_firmware | AMD EPYC™ Processors contain an information disclosure vulnerability in the Secure Encrypted Virtualization with Encrypted State (SEV-ES) and Secure Encrypted Virtualization with Secure Nested Paging (SEV-SNP). A local authenticated attacker could potentially exploit this vulnerability leading to leaking guest data by the malicious hypervisor. | 2022-02-04 | 2.1 | CVE-2020-12966 |
| apache -- gobblin | In Apache Gobblin, the Hadoop token is written to a temp file that is visible to all local users on Unix-like systems. This affects versions <= 0.15.0. Users should update to version 0.16.0 which addresses this issue. | 2022-02-04 | 2.1 | CVE-2021-36151 |
| beanstalk_console_project -- beanstalk_console | Cross-site Scripting (XSS) - Stored in Packagist ptrofimov/beanstalk_console prior to 1.7.14. | 2022-02-09 | 3.5 | CVE-2022-0539 |
| cluevo -- learning_management_system | The CLUEVO LMS, E-Learning Platform WordPress plugin before 1.8.1 does not sanitise and escape Course's module, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed | 2022-02-07 | 3.5 | CVE-2021-25029 |
| elecom -- wrc-300febk-r_firmware | Cross-site scripting vulnerability in ELECOM LAN router WRC-300FEBK-R firmware v1.13 and earlier allows an attacker on the adjacent network to inject an arbitrary script via unspecified vectors. | 2022-02-08 | 2.9 | CVE-2022-21799 |
| fleetdm -- fleet | fleet is an open source device management, built on osquery. Versions prior to 4.9.1 expose a limited ability to spoof SAML authentication with missing audience verification. This impacts deployments using SAML SSO in two specific cases: 1. A malicious or compromised Service Provider (SP) could reuse the SAML response to log into Fleet as a user -- only if the user has an account with the same email in Fleet, _and_ the user signs into the malicious SP via SAML SSO from the same Identity Provider (IdP) configured with Fleet. 2. A user with an account in Fleet could reuse a SAML response intended for another SP to log into Fleet. This is only a concern if the user is blocked from Fleet in the IdP, but continues to have an account in Fleet. If the user is blocked from the IdP entirely, this cannot be exploited. Fleet 4.9.1 resolves this issue. Users unable to upgrade should: Reduce the length of sessions on your IdP to reduce the window for malicious re-use, Limit the amount of SAML Service Providers/Applications used by user accounts with access to Fleet, and When removing access to Fleet in the IdP, delete the Fleet user from Fleet as well. | 2022-02-04 | 3.5 | CVE-2022-23600 |
| google -- android | In cmdq driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05747150; Issue ID: ALPS05747150. | 2022-02-09 | 2.1 | CVE-2022-20029 |
| google -- android | In camera driver, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05862973; Issue ID: ALPS05862973. | 2022-02-09 | 2.1 | CVE-2022-20033 |
| google -- android | In vcu driver, there is a possible information disclosure due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06171675; Issue ID: ALPS06171675. | 2022-02-09 | 2.1 | CVE-2022-20035 |
| google -- android | In Bluetooth, there is a possible information disclosure due to incorrect error handling. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS06108487; Issue ID: ALPS06108487. | 2022-02-09 | 2.1 | CVE-2022-20042 |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- android | In vow driver, there is a possible memory corruption due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS05852822; Issue ID: ALPS05852822. | 2022-02-09 | 1.9 | CVE-2022-20032 |
| google -- go-attestation | An improper input validation vulnerability in go-attestation before 0.3.3 allows local users to provide a maliciously-formed Quote over no/some PCRs, causing AKPublic.Verify to succeed despite the inconsistency. Subsequent use of the same set of PCR values in Eventlog.Verify lacks the authentication performed by quote verification, meaning a local attacker could couple this vulnerability with a maliciously-crafted TCG log in Eventlog.Verify to spoof events in the TCG log, hence defeating remotely-attested measured-boot. We recommend upgrading to Version 0.4.0 or above. | 2022-02-04 | 2.1 | CVE-2022-0317 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. The TFG dialect of TensorFlow (MLIR) makes several assumptions about the incoming `GraphDef` before converting it to the MLIR-based dialect. If an attacker changes the `SavedModel` format on disk to invalidate these assumptions and the `GraphDef` is then converted to MLIR-based IR then they can cause a crash in the Python interpreter. Under certain scenarios, heap OOB read/writes are possible. These issues have been discovered via fuzzing and it is possible that more weaknesses exist. We will patch them as they are discovered. | 2022-02-04 | 2.1 | CVE-2022-23594 |
| google -- tensorflow | Tensorflow is an Open Source Machine Learning Framework. In multiple places, TensorFlow uses `tempfile.mktemp` to create temporary files. While this is acceptable in testing, in utilities and libraries it is dangerous as a different process can create the file between the check for the filename in `mktemp` and the actual creation of the file by a subsequent operation (a TOC/TOU type of weakness). In several instances, TensorFlow was supposed to actually create a temporary directory instead of a file. This logic bug is hidden away by the `mktemp` function usage. We have patched the issue in several commits, replacing `mktemp` with the safer `mkstemp`/`mkdtemp` functions, according to the usage pattern. Users are advised to upgrade as soon as possible. | 2022-02-04 | 3.3 | CVE-2022-23563 |
| grafana -- grafana | Grafana is an open-source platform for monitoring and observability. In affected versions an attacker could serve HTML content thru the Grafana datasource or plugin proxy and trick a user to visit this HTML page using a specially crafted link and execute a Cross-site Scripting (XSS) attack. The attacker could either compromise an existing datasource for a specific Grafana instance or either set up its own public service and instruct anyone to set it up in their Grafana instance. To be impacted, all of the following must be applicable. For the data source proxy: A Grafana HTTP-based datasource configured with Server as Access Mode and a URL set, the attacker has to be in control of the HTTP server serving the URL of above datasource, and a specially crafted link pointing at the attacker controlled data source must be clicked on by an authenticated user. For the plugin proxy: A Grafana HTTP-based app plugin configured and enabled with a URL set, the attacker has to be in control of the HTTP server serving the URL of above app, and a specially crafted link pointing at the attacker controlled plugin must be clocked on by an authenticated user. For the backend plugin resource: An attacker must be able to navigate an authenticated user to a compromised plugin through a crafted link. Users are advised to update to a patched version. There are no known workarounds for this vulnerability. | 2022-02-08 | 2.1 | CVE-2022-21702 |
| grafana -- grafana | Grafana is an open-source platform for monitoring and observability. Affected versions of Grafana expose multiple API endpoints which do not properly handle user authorization. `/teams/:teamId` will allow an authenticated attacker to view unintended data by querying for the specific team ID, `/teams/:search` will allow an authenticated attacker to search for teams and see the total number of available teams, including for those teams that the user does not have access to, and `/teams/:teamId/members` when editors_can_admin flag is enabled, an authenticated attacker can see unintended data by querying for the specific team | 2022-02-08 | 3.5 | CVE-2022-21713 |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| | ID. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue. | | | |
| gtranslate -- translate_wordpress_with_gtranslate | The Translate WordPress with GTranslate WordPress plugin before 2.9.7 does not sanitise and escape the body parameter in the url_addon/gtranslate-email.php file before outputting it back in the page, leading to a Reflected Cross-Site Scripting issue. Note: exploitation of the issue requires knowledge of the NONCE_SALT and NONCE_KEY | 2022-02-07 | 2.6 | CVE-2021-25103 |
| ivorysearch -- ivory_search | The Ivory Search WordPress plugin before 5.4.1 does not escape some of the Form settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. | 2022-02-07 | 3.5 | CVE-2021-25105 |
| laracom_project -- laracom | Unrestricted Upload of File with Dangerous Type in Packagist jsdecena/laracom prior to v2.0.9. | 2022-02-04 | 3.5 | CVE-2022-0472 |
| linux -- linux_kernel | An issue was discovered in fs/nfs/dir.c in the Linux kernel before 5.16.5. If an application sets the O_DIRECTORY flag, and tries to open a regular file, nfs_atomic_open() performs a regular lookup. If a regular file is found, ENOTDIR should occur, but the server instead returns uninitialized data in the file descriptor. | 2022-02-04 | 1.9 | CVE-2022-24448 |
| linux -- linux_kernel | A vulnerability was found in the Linux kernel's eBPF verifier when handling internal data structures. Internal memory locations could be returned to userspace. A local attacker with the permissions to insert eBPF code to the kernel can use this to leak internal kernel memory details defeating some of the exploit mitigations in place for the kernel. This flaws affects kernel versions < v5.16-rc6 | 2022-02-04 | 2.1 | CVE-2022-0264 |
| linux -- linux_kernel | A use-after-free vulnerability was found in rtsx_usb_ms_drv_remove in drivers/memstick/host/rtsx_usb_ms.c in memstick in the Linux kernel. In this flaw, a local attacker with a user privilege may impact system Confidentiality. This flaw affects kernel versions prior to 5.14 rc1. | 2022-02-04 | 2.1 | CVE-2022-0487 |
| livehelperchat -- live_helper_chat | Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v. | 2022-02-06 | 3.5 | CVE-2022-0502 |
| microweber -- microweber | Cross-site Scripting (XSS) - Stored in Packagist microweber/microweber prior to 1.2.11. | 2022-02-08 | 3.5 | CVE-2022-0506 |
| nvidia -- gpu_display_driver | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel driver, where improper handling of insufficient permissions or privileges may allow an unprivileged local user limited write access to protected memory, which can lead to denial of service. | 2022-02-07 | 3.6 | CVE-2022-21813 |
| nvidia -- gpu_display_driver | NVIDIA GPU Display Driver for Linux contains a vulnerability in the kernel driver package, where improper handling of insufficient permissions or privileges may allow an unprivileged local user limited write access to protected memory, which can lead to denial of service. | 2022-02-07 | 3.6 | CVE-2022-21814 |
| pimcore -- pimcore | Cross-site Scripting (XSS) - Reflected in Packagist pimcore/pimcore prior to 10.3.1. | 2022-02-08 | 3.5 | CVE-2022-0510 |
| pimcore -- pimcore | Cross-site Scripting (XSS) - Stored in Packagist pimcore/pimcore prior to 10.3.1. | 2022-02-08 | 3.5 | CVE-2022-0509 |
| premio -- mystickyelements | The All-in-one Floating Contact Form, Call, Chat, and 50+ Social Icon Tabs WordPress plugin before 2.0.4 was vulnerable to reflected XSS on the my-sticky-elements-leads admin page. | 2022-02-07 | 3.5 | CVE-2022-0148 |
| schneider-electric -- ecostruxure_power_monitoring_expert | A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists that could allow an authenticated attacker to view data, change settings, or impact availability of the software when the user visits a page containing the injected payload. Affected Product: EcoStruxure Power Monitoring Expert (Versions 2020 and prior) | 2022-02-04 | 3.5 | CVE-2022-22804 |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| std42 -- elfinder | Studio 42 elFinder through 2.1.31 allows XSS via an SVG document. | 2022-02-08 | 3.5 | CVE-2021-45919 |
| supportcandy -- supportcandy | The SupportCandy WordPress plugin before 2.2.7 does not validate and escape the page attribute of its shortcode, which could allow users with a role as low as Contributor to perform Cross-Site Scripting attacks | 2022-02-07 | 3.5 | CVE-2021-24880 |
| tastyigniter -- tastyigniter | A Cross-Site Scripting (XSS) vulnerability exists within the 3.2.2 version of TastyIgniter. The "items%5B0%5D%5Bpath%5D" parameter of a request made to /admin/allergens/edit/1 is vulnerable. | 2022-02-09 | 3.5 | CVE-2022-23378 |
| trendmicro -- worry-free_business_security | A security out-of-bounds read information disclosure vulnerability in Trend Micro Worry-Free Business Security Server could allow a local attacker to send garbage data to a specific named pipe and crash the server. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. | 2022-02-04 | 3.6 | CVE-2022-23805 |
| wire -- wire-webapp | Wire webapp is a web client for the wire messaging protocol. In versions prior to 2022-01-27-production.0 expired ephemeral messages were not reliably removed from local chat history of Wire Webapp. In versions before 2022-01-27-production.0 ephemeral messages and assets might still be accessible through the local search functionality. Any attempt to view one of these message in the chat view will then trigger the deletion. This issue only affects locally stored messages. On premise instances of wire-webapp need to be updated to 2022-01-27-production.0, so that their users are no longer affected. There are no known workarounds for this issue. | 2022-02-04 | 2.1 | CVE-2022-23605 |
| wpeka -- wplegalpages | The Privacy Policy Generator, Terms & Conditions Generator WordPress Plugin : WPLegalPages WordPress plugin before 2.7.1 does not check for authorisation and has a flawed CSRF logic when saving its settings, allowing any authenticated users, such as subscriber, to update them. Furthermore, due to the lack of sanitisation and escaping, it could lead to Stored Cross-Site Scripting | 2022-02-07 | 3.5 | CVE-2021-25106 |
| xwiki -- xwiki | XWiki is a generic wiki platform offering runtime services for applications built on top of it. When using default XWiki configuration, it's possible for an attacker to upload an SVG containing a script executed when executing the download action on the file. This problem has been patched so that the default configuration doesn't allow to display the SVG files in the browser. Users are advised to update or to disallow uploads of SVG files. | 2022-02-04 | 3.5 | CVE-2021-43841 |
| drupal -- drupal | Cross-site Scripting (XSS) vulnerability in Drupal core's sanitization API fails to properly filter cross-site scripting under certain circumstances. This issue affects: Drupal Core 9.1.x versions prior to 9.1.7; 9.0.x versions prior to 9.0.12; 8.9.x versions prior to 8.9.14; 7.x versions prior to 7.80. | 2022-02-11 | 2.6 | CVE-2020-13672 |
| factorfx -- ocs_inventory | OCS Inventory 2.9.1 is affected by Cross Site Scripting (XSS). To exploit the vulnerability, the attacker needs to manipulate the name of some device on your computer, such as a printer, replacing the device name with some malicious code that allows the execution of Stored Cross-site Scripting (XSS). | 2022-02-11 | 3.5 | CVE-2021-46355 |
| google -- android | PendingIntent hijacking vulnerability in KnoxPrivacyNoticeReceiver prior to SMR Feb-2022 Release 1 allows local attackers to access media files without permission via implicit Intent. | 2022-02-11 | 3.6 | CVE-2022-23427 |
| google -- android | Logging of excessive data vulnerability in telephony prior to SMR Feb-2022 Release 1 allows privileged attackers to get Cell Location Information through log of user device. | 2022-02-11 | 2.1 | CVE-2022-22291 |
| google -- android | In TBD of TBD, there is a possible out of bounds read due to TBD. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-206039140References: N/A | 2022-02-11 | 2.1 | CVE-2021-39688 |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| google -- android | In HandleTransactionIoEvent of actuator_driver.cc, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-204421047References: N/A | 2022-02-11 | 2.1 | CVE-2021-39687 |
| google -- android | In extract of MediaMetricsItem.h, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-204445255 | 2022-02-11 | 2.1 | CVE-2021-39666 |
| google -- android | In clear_data_dlg_text of strings.xml, there is a possible situation when "Clear storage" functionality sets up the wrong security/privacy expectations due to a misleading message. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12Android ID: A-193890833 | 2022-02-11 | 2.1 | CVE-2021-39631 |
| google -- android | In isServiceDistractionOptimized of CarPackageManagerService.java, there is a possible disclosure of installed packages due to side channel information disclosure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-180418334 | 2022-02-11 | 2.1 | CVE-2021-0524 |
| google -- android | A vulnerability using PendingIntent in DeX Home and DeX for PC prior to SMR Feb-2022 Release 1 allows attackers to access files with system privilege. | 2022-02-11 | 3.6 | CVE-2022-23426 |
| google -- android | An improper boundary check in audio hal service prior to SMR Feb-2022 Release 1 allows attackers to read invalid memory and it leads to application crash. | 2022-02-11 | 3.6 | CVE-2022-23429 |
| google -- android | In LoadedPackage::Load of LoadedArsc.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure when parsing an APK file with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-12Android ID: A-203938029 | 2022-02-11 | 1.9 | CVE-2021-39664 |
| linux -- linux_kernel | An issue was discovered in the Linux kernel before 5.16.5. There is a memory leak in yam_siocdevprivate in drivers/net/hamradio/yam.c. | 2022-02-11 | 2.1 | CVE-2022-24959 |
| najeebmedia -- ppom_for_woocommerce | The PPOM for WooCommerce WordPress plugin before 24.0 does not have authorisation and CSRF checks in the ppom_settings_panel_action AJAX action, allowing any authenticated to call it and set arbitrary settings. Furthermore, due to the lack of sanitisation and escaping, it could lead to Stored XSS issues | 2022-02-14 | 3.5 | CVE-2021-25018 |
| projeqtor -- projeqtor | A Cross Site Scripting (XSS) vulnerability exists in Projeqtor 9.3.1 via /projeqtor/tool/saveAttachment.php, which allows an attacker to upload a SVG file containing malicious JavaScript code. | 2022-02-11 | 3.5 | CVE-2021-42940 |
| s-cart -- s-cart | A Directory Traversal vulnerability exists in S-Cart 6.7 via download in sc-admin/backup. | 2022-02-11 | 2.1 | CVE-2021-44111 |
| samsung -- bixby | A vulnerability using PendingIntent in Bixby Vision prior to versions 3.7.60.8 in Android S(12), 3.7.50.6 in Andorid R(11) and below allows attackers to execute privileged action by hijacking and modifying the intent. | 2022-02-11 | 2.1 | CVE-2022-23434 |
| tcman -- gim | The m_txtNom y m_txtCognoms parameters in TCMAN GIM v8.01 allow an attacker to perform persistent XSS attacks. This vulnerability could be used to carry out a number of browser-based attacks including browser hijacking or theft of sensitive data. | 2022-02-11 | 3.5 | CVE-2021-4046 |

# Low Vulnerabilities

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| themify -- portfolio_post | Themify Portfolio Post WordPress plugin before 1.1.7 does not sanitise and escape the num_of_pages parameter before outputting it back the response of the themify_create_popup_page_pagination AJAX action (available to any authenticated user), leading to a Reflected Cross-Site Scripting | 2022-02-14 | 3.5 | CVE-2022-0200 |
| vicidial -- vicidial | Vicidial 2.14-783a was discovered to contain a cross-site scripting (XSS) vulnerability via the input tabs. | 2022-02-15 | 3.5 | CVE-2021-46557 |
| wp_photo_album_plus_project -- wp_photo_album_plus | The WP Photo Album Plus WordPress plugin before 8.0.10 was vulnerable to Stored Cross-Site Scripting (XSS). Error log content was handled improperly, therefore any user, even unauthenticated, could cause arbitrary javascript to be executed in the admin panel. | 2022-02-14 | 3.5 | CVE-2021-25115 |
| wpchill -- remove_footer_credit | The Remove Footer Credit WordPress plugin before 1.0.11 does properly sanitise its settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed. | 2022-02-14 | 3.5 | CVE-2021-25050 |