SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 09 February 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-21961	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.	10.0	More Details
CVE-2021-21960	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.	10.0	More Details
CVE-2021-43928	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 20211105-10315 allows remote authenticated users to execute arbitrary commands via unspecified vectors.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24148	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.	9.8	More Details
CVE-2022-24150	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.	9.8	More Details
CVE-2022-24165	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.	9.8	More Details
CVE-2022-24167	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.	9.8	More Details
CVE-2022-24168	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.	9.8	More Details
CVE-2022-24170	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.	9.8	More Details
CVE-2022-24171	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.	9.8	More Details
CVE-2021-44978	iCMS <= 8.0.0 allows users to add and render a comtom template, which has a SSTI vulnerability which causes remote code execution.	9.8	More Details
CVE-2022-24259	An incorrect check in the component cdr.php of Voipmonitor GUI before v24.96 allows unauthenticated attackers to escalate privileges via a crafted request.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24260	A SQL injection vulnerability in Voipmonitor GUI before v24.96 allows attackers to escalate privileges to the Administrator level.	9.8	More Details
CVE-2021-29393	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.	9.8	More Details
CVE-2021-29396	Systemic Insecure Permissions in Northstar Technologies Inc NorthStar Club Management 6.3 allows remote unauthenticated users to use various functionalities without authentication.	9.8	More Details
CVE-2022-23329	A vulnerability in ${"freemarker.template.utility.Execute"?new() of UJCMS Jspxcms v10.2.0 allows attackers to execute arbitrary commands via uploading malicious files.	9.8	More Details
CVE-2022-24300	Minetest before 5.4.0 allows attackers to add or modify arbitrary meta fields of the same item stack as saved user input, aka ItemStack meta injection.	9.8	More Details
CVE-2021-46456	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.	9.8	More Details
CVE-2021-36152	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.	9.8	More Details
CVE-2022-22987	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.	9.8	More Details
CVE-2022-23379	Emlog v6.0 was discovered to contain a SQL injection vulnerability via the $TagID parameter of getblogidsfromtagid().	9.8	More Details
CVE-2021-38172	perM 0.4.0 has a Buffer Overflow related to strncpy. (Debian initially fixed this in 0.4.0-7.)	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-20004	A flaw was found in StarWind iSCSI target. StarWind service does not limit client connections and allocates memory on each connection attempt. An attacker could create a denial of service state by trying to connect a non-existent target multiple times. This affects iSCSI SAN (Windows Native) Version 6.0, build 2013-01-16.	9.8	More Details
CVE-2021-41816	CGI.escape_html in Ruby before 2.7.5 and 3.x before 3.0.3 has an integer overflow and resultant buffer overflow via a long string on platforms (such as Windows) where size_t and long have different numbers of bytes. This also affects the CGI gem before 0.3.1 for Ruby.	9.8	More Details
CVE-2022-22831	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.	9.8	More Details
CVE-2022-22832	An issue was discovered in Servisnet Tessa 0.0.2. Authorization data is available via an unauthenticated /data-service/users/ request.	9.8	More Details
CVE-2022-24552	A flaw was found in the REST API in StarWind Stack. REST command, which manipulates a virtual disk, doesn't check input parameters. Some of them go directly to bash as part of a script. An attacker with non-root user access can inject arbitrary data into the command that will be executed with root privileges. This affects StarWind SAN and NAS v0.2 build 1633.	9.8	More Details
CVE-2021-25114	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	9.8	More Details
CVE-2022-23340	Joplin 2.6.10 allows remote attackers to execute system commands through malicious code in user search results.	9.8	More Details
CVE-2021-45327	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.	9.8	More Details
CVE-2021-46457	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.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24144	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.	9.8	More Details
CVE-2021-46455	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.	9.8	More Details
CVE-2021-45987	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.	9.8	More Details
CVE-2021-39070	IBM Security Verify Access 10.0.0.0, 10.0.1.0 and 10.0.2.0 with the advanced access control authentication service enabled could allow an attacker to authenticate as any user on the system. IBM X-Force ID: 215353.	9.8	More Details
CVE-2021-42637	PrinterLogic Web Stack versions 19.1.1.13 SP9 and below use user-controlled input to craft a URL, resulting in a Server Side Request Forgery (SSRF) vulnerability.	9.8	More Details
CVE-2022-24307	Mastodon before 3.3.2 and 3.4.x before 3.4.6 has incorrect access control because it does not compact incoming signed JSON-LD activities. (JSON-LD signing has been supported since version 1.6.0.)	9.8	More Details
CVE-2021-44247	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.	9.8	More Details
CVE-2021-44880	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.	9.8	More Details
CVE-2021-44881	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.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44882	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.	9.8	More Details
CVE-2021-45733	TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to contain a command injection vulnerability in the function NTPSyncWithHost. This vulnerability allows attackers to execute arbitrary commands via the parameter host_time.	9.8	More Details
CVE-2021-45738	TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to contain a command injection vulnerability in the function UploadFirmwareFile. This vulnerability allows attackers to execute arbitrary commands via the parameter FileName.	9.8	More Details
CVE-2021-45740	TOTOLINK A720R v4.1.5cu.470_B20200911 was discovered to contain a stack overflow in the setWiFiWpsStart function. This vulnerability allows attackers to cause a Denial of Service (DoS) via the pin parameter.	9.8	More Details
CVE-2021-46454	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.	9.8	More Details
CVE-2021-45742	TOTOLINK A720R v4.1.5cu.470_B20200911 was discovered to contain a command injection vulnerability in the "Main" function. This vulnerability allows attackers to execute arbitrary commands via the QUERY_STRING parameter.	9.8	More Details
CVE-2021-45986	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.	9.8	More Details
CVE-2022-0139	Use After Free in GitHub repository radareorg/radare2 prior to 5.6.0.	9.8	More Details
CVE-2021-45990	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.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46230	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.	9.8	More Details
CVE-2021-46453	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.	9.8	More Details
CVE-2021-46452	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.	9.8	More Details
CVE-2021-45998	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.	9.8	More Details
CVE-2021-46232	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.	9.8	More Details
CVE-2021-46231	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.	9.8	More Details
CVE-2021-46233	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.	9.8	More Details
CVE-2021-46229	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.	9.8	More Details
CVE-2021-46228	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.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46227	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.	9.8	More Details
CVE-2021-46226	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.	9.8	More Details
CVE-2022-21241	Cross-site scripting vulnerability in CSV+ prior to 0.8.1 allows a remote unauthenticated attacker to inject an arbitrary script or an arbitrary OS command via a specially crafted CSV file that contains HTML a tag.	9.6	More Details
CVE-2021-42833	A Use of Hardcoded Credentials vulnerability exists in AquaView versions 1.60, 7.x, and 8.x that could allow an authenticated local attacker to manipulate users and system settings.	9.3	More Details
CVE-2022-21817	NVIDIA Omniverse Launcher contains a Cross-Origin Resource Sharing (CORS) vulnerability which can allow an unprivileged remote attacker, if they can get user to browse malicious site, to acquire access tokens allowing them to access resources in other security domains, which may lead to code execution, escalation of privileges, and impact to confidentiality and integrity.	9.3	More Details
CVE-2021-21965	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.	9.3	More Details
CVE-2022-0365	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.	9.1	More Details
CVE-2022-23357	mozilo2.0 was discovered to be vulnerable to directory traversal attacks via the parameter curent_dir.	9.1	More Details
CVE-2021-42640	PrinterLogic Web Stack versions 19.1.1.13 SP9 and below are vulnerable to an Insecure Direct Object Reference (IDOR) vulnerability that allows an unauthenticated attacker to reassign drivers for any printer.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24043	A missing bound check in RTCP flag parsing code prior to WhatsApp for Android v2.21.23.2, WhatsApp Business for Android v2.21.23.2, WhatsApp for iOS v2.21.230.6, WhatsApp Business for iOS 2.21.230.7, and WhatsApp Desktop v2.2145.0 could have allowed an out-of-bounds heap read if a user sent a malformed RTCP packet during an established call.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-23566	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.	8.8	More Details
CVE-2020-7534	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)	8.8	More Details
CVE-2021-46398	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.	8.8	More Details
CVE-2022-24262	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.	8.8	More Details
CVE-2022-23873	Victor CMS v1.0 was discovered to contain a SQL injection vulnerability that allows attackers to inject arbitrary commands via 'user_firstname' parameter.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23594	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.	8.8	More Details
CVE-2021-45326	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.	8.8	More Details
CVE-2022-22723	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)	8.8	More Details
CVE-2022-23561	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.	8.8	More Details
CVE-2022-23331	In DataEase v1.6.1, an authenticated user can gain unauthorized access to all user information and can change the administrator password.	8.8	More Details
CVE-2022-21173	Hidden functionality vulnerability in ELECOM LAN routers (WRH-300BK3 firmware v1.05 and earlier, WRH-300WH3 firmware v1.05 and earlier, WRH-300BK3-S firmware v1.05 and earlier, WRH-300DR3-S firmware v1.05 and earlier, WRH-300LB3-S firmware v1.05 and earlier, WRH-300PN3-S firmware v1.05 and earlier, WRH-300WH3-S firmware v1.05 and earlier, and WRH-300YG3-S firmware v1.05 and earlier) allows an attacker on the adjacent network to execute an arbitrary OS command via unspecified vectors.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40420	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.	8.8	More Details
CVE-2022-23560	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.	8.8	More Details
CVE-2021-24879	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.	8.8	More Details
CVE-2022-23559	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.	8.8	More Details
CVE-2022-24450	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.	8.8	More Details
CVE-2021-45268	A Cross Site Request Forgery (CSRF) vulnerability exists in Backdrop CMS 1.20, which allows Remote Attackers to gain Remote Code Execution (RCE) on the Hosting Webserver via uploading a maliciously add-on with crafted PHP file. NOTE: the vendor disputes this because the attack requires a session cookie of a high-privileged authenticated user who is entitled to install arbitrary add-ons	8.8	More Details
CVE-2022-23330	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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22725	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)	8.8	More Details
CVE-2022-22727	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)	8.8	More Details
CVE-2022-22689	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.	8.8	More Details
CVE-2022-23614	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.	8.8	More Details
CVE-2022-22150	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 vulnerability. Exploitation is also possible if a user visits a specially-crafted, malicious site if the browser plugin extension is enabled.	8.8	More Details
CVE-2021-39280	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.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23574	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.	8.8	More Details
CVE-2022-24551	A flaw was found in StarWind Stack. The endpoint for setting a new password doesn’t check the current username and old password. An attacker could reset any local user password (including system/administrator user) using any available user This affects StarWind SAN and NAS v0.2 build 1633.	8.8	More Details
CVE-2021-4154	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.	8.8	More Details
CVE-2022-22509	In Phoenix Contact FL SWITCH Series 2xxx in version 3.00 an incorrect privilege assignment allows an low privileged user to enable full access to the device configuration.	8.8	More Details
CVE-2022-23587	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.	8.8	More Details
CVE-2022-0366	An authenticated and authorized agent user could potentially gain administrative access via an SQLi vulnerability to Capsule8 Console between versions 4.6.0 and 4.9.1.	8.8	More Details
CVE-2021-41018	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWeb version 6.4.1 and below, 6.3.15 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39044	IBM Financial Transaction Manager 3.2.4 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 214210.	8.8	More Details
CVE-2021-39066	IBM Financial Transaction Manager 3.2.4 does not invalidate session any existing session identifier gives an attacker the opportunity to steal authenticated sessions. IBM X-Force ID: 215040.	8.8	More Details
CVE-2021-43073	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWeb version 6.4.1 and 6.4.0, version 6.3.15 and below, version 6.2.6 and below allows attacker to execute unauthorized code or commands via crafted HTTP requests.	8.8	More Details
CVE-2022-0484	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.	8.8	More Details
CVE-2021-40401	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.	8.6	More Details
CVE-2022-23626	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.	8.5	More Details
CVE-2021-22284	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.	8.4	More Details
CVE-2021-21968	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.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2013-20003	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.	8.3	More Details
CVE-2022-23609	iTunesRPC-Remastered is a Discord Rich Presence for iTunes on Windows utility. In affected versions iTunesRPC-Remastered did not properly sanitize user input used to remove files leading to file deletion only limited by the process permissions. Users are advised to upgrade as soon as possible.	8.3	More Details
CVE-2022-0218	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.	8.3	More Details
CVE-2021-3835	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	8.2	More Details
CVE-2022-24129	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.	8.2	More Details
CVE-2021-23470	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 vulnerability derives from an incomplete fix in https://security.snyk.io/vuln/SNYK-JS-PUTILMERGE-1317077	8.2	More Details
CVE-2022-24069	An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.0 before 05.08.41, 5.1 before 05.16.29, 5.2 before 05.26.29, 5.3 before 05.35.29, 5.4 before 05.43.29, and 5.5 before 05.51.29. An SMM callout vulnerability allows an attacker to hijack the execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.	8.2	More Details
CVE-2021-43615	An issue was discovered in HddPassword in Insyde InsydeH2O with kernel 5.1 before 05.16.23, 5.2 before 05.26.23, 5.3 before 05.35.23, 5.4 before 05.43.22, and 5.5 before 05.51.22. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41841	An issue was discovered in AhciBusDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. There is an SMM callout that allows an attacker to access the System Management Mode and execute arbitrary code. This occurs because of Inclusion of Functionality from an Untrusted Control Sphere.	8.2	More Details
CVE-2021-3861	The RNDIS USB device class includes a buffer overflow vulnerability. 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-hvfp-w4h8-gxvj	8.2	More Details
CVE-2021-33627	An issue was discovered in Insyde InsydeH2O Kernel 5.0 before 05.09.11, 5.1 before 05.17.11, 5.2 before 05.27.11, 5.3 before 05.36.11, 5.4 before 05.44.11, and 5.5 before 05.52.11 affecting FwBlockServiceSmm. Software SMI services that use the Communicate() function of the EFI_SMM_COMMUNICATION_PROTOCOL do not check whether the address of the buffer is valid, which allows use of SMRAM, MMIO, or OS kernel addresses.	8.2	More Details
CVE-2022-24031	An issue was discovered in NvmExpressDxe in Insyde InsydeH2O with kernel 5.1 through 5.5. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.	8.2	More Details
CVE-2021-41837	An issue was discovered in AhciBusDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. Because of an Untrusted Pointer Dereference that causes SMM memory corruption, an attacker may be able to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.	8.2	More Details
CVE-2021-41838	An issue was discovered in SdHostDriver in the kernel 5.0 through 5.5 in Insyde InsydeH2O. There is an SMM callout that allows an attacker to access the System Management Mode and execute arbitrary code. This occurs because of a Numeric Range Comparison Without a Minimum Check.	8.2	More Details
CVE-2021-41839	An issue was discovered in NvmExpressDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. Because of an Untrusted Pointer Dereference that causes SMM memory corruption, an attacker may be able to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43323	An issue was discovered in UsbCoreDxe in Insyde InsydeH2O with kernel 5.5 before 05.51.45, 5.4 before 05.43.45, 5.3 before 05.35.45, 5.2 before 05.26.45, 5.1 before 05.16.45, and 5.0 before 05.08.45. An SMM callout vulnerability allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.	8.2	More Details
CVE-2021-42554	An issue was discovered in Insyde InsydeH2O with Kernel 5.0 before 05.08.42, Kernel 5.1 before 05.16.42, Kernel 5.2 before 05.26.42, Kernel 5.3 before 05.35.42, Kernel 5.4 before 05.42.51, and Kernel 5.5 before 05.50.51. An SMM memory corruption vulnerability in FvbServicesRuntimeDxe allows a possible attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.	8.2	More Details
CVE-2021-42113	An issue was discovered in StorageSecurityCommandDxe in Insyde InsydeH2O with Kernel 5.1 before 05.14.28, Kernel 5.2 before 05.24.28, and Kernel 5.3 before 05.32.25. An SMM callout vulnerability allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.	8.2	More Details
CVE-2021-42060	An issue was discovered in Insyde InsydeH2O Kernel 5.0 through 05.08.41, Kernel 5.1 through 05.16.41, Kernel 5.2 before 05.23.22, and Kernel 5.3 before 05.32.22. An Int15ServiceSmm SMM callout vulnerability allows an attacker to hijack execution flow of code running in System Management Mode. Exploiting this issue could lead to escalating privileges to SMM.	8.2	More Details
CVE-2021-41840	An issue was discovered in NvmExpressDxe in the kernel 5.0 through 5.5 in Insyde InsydeH2O. There is an SMM callout that allows an attacker to access the System Management Mode and execute arbitrary code. This occurs because of Inclusion of Functionality from an Untrusted Control Sphere.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21728	Tensorflow is an Open Source Machine Learning Framework. The implementation of shape inference for `ReverseSequence` does not fully validate the value of `batch_dim` and can result in a heap OOB read. There is a check to make sure the value of `batch_dim` does not go over the rank of the input, but there is no check for negative values. Negative dimensions are allowed in some cases to mimic Python's negative indexing (i.e., indexing from the end of the array), however if the value is too negative then the implementation of `Dim` would access elements before the start of an array. 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.	8.1	More Details
CVE-2021-42753	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability [CWE-22] in FortiWeb management interface 6.4.1 and below, 6.3.15 and below, 6.2.x, 6.1.x, 6.0.x, 5.9.x and 5.8.x may allow an authenticated attacker to perform an arbitrary file and directory deletion in the device filesystem.	8.1	More Details
CVE-2018-25029	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.	8.1	More Details
CVE-2022-23623	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`.	8.1	More Details
CVE-2021-43145	With certain LDAP configurations, Zammad 5.0.1 was found to be vulnerable to unauthorized access with existing user accounts.	8.1	More Details
CVE-2022-23624	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`.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21726	Tensorflow is an Open Source Machine Learning Framework. The implementation of `Dequantize` does not fully validate the value of `axis` and can result in heap OOB accesses. The `axis` argument can be `-1` (the default value for the optional argument) or any other positive value at most the number of dimensions of the input. Unfortunately, the upper bound is not checked and this results in reading past the end of the array containing the dimensions of the input tensor. 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.	8.1	More Details
CVE-2022-23611	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.	8.1	More Details
CVE-2022-23592	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.	8.1	More Details
CVE-2021-21959	A misconfiguration exists in the MQTTS functionality of Sealevel Systems, Inc. SeaConnect 370W v1.3.34. This misconfiguration significantly simplifies a man-in-the-middle attack, which directly leads to control of device functionality.	8.1	More Details
CVE-2021-21970	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.	8.1	More Details
CVE-2021-21962	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.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21969	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.	8.1	More Details
CVE-2022-21730	Tensorflow is an Open Source Machine Learning Framework. The implementation of `FractionalAvgPoolGrad` does not consider cases where the input tensors are invalid allowing an attacker to read from outside of bounds of heap. 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.	8.1	More Details
CVE-2021-44903	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.	7.8	More Details
CVE-2022-23613	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.	7.8	More Details
CVE-2021-44899	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.	7.8	More Details
CVE-2020-12891	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.	7.8	More Details
CVE-2021-44900	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.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29219	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.	7.8	More Details
CVE-2021-44204	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	7.8	More Details
CVE-2022-23946	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.	7.8	More Details
CVE-2022-23947	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.	7.8	More Details
CVE-2022-24115	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	7.8	More Details
CVE-2021-44901	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.	7.8	More Details
CVE-2022-24113	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	7.8	More Details
CVE-2022-0443	Use After Free in GitHub repository vim/vim prior to 8.2.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0523	Use After Free in GitHub repository radareorg/radare2 prior to 5.6.2.	7.8	More Details
CVE-2021-41016	A improper neutralization of special elements used in a command ('command injection') in Fortinet FortiExtender version 7.0.1 and below, 4.2.3 and below, 4.1.7 and below allows an authenticated attacker to execute privileged shell commands via CLI commands including special characters	7.8	More Details
CVE-2022-0520	Use After Free in NPM radare2.js prior to 5.6.2.	7.8	More Details
CVE-2022-23263	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	7.7	More Details
CVE-2022-24348	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.	7.7	More Details
CVE-2022-23584	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.	7.6	More Details
CVE-2022-23562	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.	7.6	More Details
CVE-2022-23558	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.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21727	Tensorflow is an Open Source Machine Learning Framework. The implementation of shape inference for `Dequantize` is vulnerable to an integer overflow weakness. The `axis` argument can be `-1` (the default value for the optional argument) or any other positive value at most the number of dimensions of the input. Unfortunately, the upper bound is not checked, and, since the code computes `axis + 1`, an attacker can trigger an integer overflow. 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.	7.6	More Details
CVE-2022-21740	Tensorflow is an Open Source Machine Learning Framework. The implementation of `SparseCountSparseOutput` is vulnerable to a heap overflow. 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.	7.6	More Details
CVE-2022-21736	Tensorflow is an Open Source Machine Learning Framework. The implementation of `SparseTensorSliceDataset` has an undefined behavior: under certain condition it can be made to dereference a `nullptr` value. The 3 input arguments to `SparseTensorSliceDataset` represent a sparse tensor. However, there are some preconditions that these arguments must satisfy but these are not validated in the implementation. 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.	7.6	More Details
CVE-2022-23573	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.	7.6	More Details
CVE-2022-21193	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.	7.5	More Details
CVE-2021-22286	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.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45734	TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to contain a stack overflow in the function setUrlFilterRules. This vulnerability allows attackers to cause a Denial of Service (DoS) via the url parameter.	7.5	More Details
CVE-2021-44866	An issue was discovered in Online-Movie-Ticket-Booking-System 1.0. The file about.php does not perform input validation on the 'id' paramter. An attacker can append SQL queries to the input to extract sensitive information from the database.	7.5	More Details
CVE-2021-45325	Server Side Request Forgery (SSRF) vulneraility exists in Gitea before 1.7.0 using the OpenID URL.	7.5	More Details
CVE-2021-45735	TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to use the HTTP protocol for authentication into the admin interface, allowing attackers to intercept user credentials via packet capture software.	7.5	More Details
CVE-2020-12965	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.	7.5	More Details
CVE-2022-24121	SQL Injection vulnerability discovered in Unified Office Total Connect Now that would allow an attacker to extract sensitive information through a cookie parameter.	7.5	More Details
CVE-2021-44246	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.	7.5	More Details
CVE-2022-24030	An issue was discovered in AhciBusDxe in Insyde InsydeH2O with kernel 5.1 through 5.5. An SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.	7.5	More Details
CVE-2021-24839	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.	7.5	More Details
CVE-2022-23833	An issue was discovered in MultiPartParser in Django 2.2 before 2.2.27, 3.2 before 3.2.12, and 4.0 before 4.0.2. Passing certain inputs to multipart forms could result in an infinite loop when parsing files.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22285	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.	7.5	More Details
CVE-2022-24145	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.	7.5	More Details
CVE-2021-22288	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.	7.5	More Details
CVE-2021-43522	An issue was discovered in Insyde InsydeH2O with kernel 5.1 through 2021-11-08, 5.2 through 2021-11-08, and 5.3 through 2021-11-08. A StorageSecurityCommandDxe SMM memory corruption vulnerability allows an attacker to write fixed or predictable data to SMRAM. Exploiting this issue could lead to escalating privileges to SMM.	7.5	More Details
CVE-2022-0524	Business Logic Errors in GitHub repository publify/publify prior to 9.2.7.	7.5	More Details
CVE-2022-23206	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.	7.5	More Details
CVE-2007-20001	A flaw was found in StarWind iSCSI target. An attacker could script standard iSCSI Initiator operation(s) to exhaust the StarWind service socket, which could lead to denial of service. This affects iSCSI SAN (Windows Native) Version 3.2.2 build 2007-02-20.	7.5	More Details
CVE-2022-22510	Codesys Profinet in version V4.2.0.0 is prone to null pointer dereference that allows a denial of service (DoS) attack of an unauthenticated user via SNMP.	7.5	More Details
CVE-2021-42641	PrinterLogic Web Stack versions 19.1.1.13 SP9 and below are vulnerable to an Insecure Direct Object Reference (IDOR) vulnerability that allows an unauthenticated attacker to disclose the username and email address of all users.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42642	PrinterLogic Web Stack versions 19.1.1.13 SP9 and below are vulnerable to an Insecure Direct Object Reference (IDOR) vulnerability that allows an unauthenticated attacker to disclose the plaintext console username and password for a printer.	7.5	More Details
CVE-2022-22833	An issue was discovered in Servisnet Tessa 0.0.2. An attacker can obtain sensitive information via a /js/app.js request.	7.5	More Details
CVE-2020-5953	A vulnerability exists in System Management Interrupt (SWSMI) handler of InsydeH2O UEFI Firmware code located in SWSMI handler that dereferences gRT (EFI_RUNTIME_SERVICES) pointer to call a GetVariable service, which is located outside of SMRAM. This can result in code execution in SMM (escalating privilege from ring 0 to ring -2).	7.5	More Details
CVE-2022-22722	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)	7.5	More Details
CVE-2021-33625	An issue was discovered in Kernel 5.x in Insyde InsydeH2O, affecting HddPassword. Software SMI services that use the Communicate() function of the EFI_SMM_COMMUNICATION_PROTOCOL do not check whether the address of the buffer is valid, which allows use of SMRAM, MMIO, or OS kernel addresses.	7.5	More Details
CVE-2021-38960	IBM OPENBMC OP920, OP930, and OP940 could allow an unauthenticated user to obtain sensitive information. IBM X-Force ID: 212047.	7.5	More Details
CVE-2022-23320	XMPie uStore 12.3.7244.0 allows for administrators to generate reports based on raw SQL queries. Since the application ships with default administrative credentials, an attacker may authenticate into the application and exfiltrate sensitive information from the database.	7.5	More Details
CVE-2021-46359	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.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-32732	### 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)	7.5	More Details
CVE-2022-24146	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.	7.5	More Details
CVE-2022-23591	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.	7.5	More Details
CVE-2021-46389	IIPImage High Resolution Streaming Image Server prior to commit 882925b295a80ec992063deffc2a3b0d803c3195 is affected by an integer overflow in iipsrv.fcgi through malformed HTTP query parameters.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22724	A CWE-400: Uncontrolled Resource Consumption vulnerability exists that could cause a denial of service on ports 80 (HTTP) and 502 (Modbus), when sending a large number of TCP RST or FIN packets to any open TCP port of the PLC. Affected Product: Modicon M340 CPUs: BMXP34 (All Versions)	7.5	More Details
CVE-2021-45736	TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to contain a stack overflow in the function setL2tpServerCfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via the eip, sip, server parameters.	7.5	More Details
CVE-2022-24142	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.	7.5	More Details
CVE-2022-24172	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.	7.5	More Details
CVE-2022-24169	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.	7.5	More Details
CVE-2022-24166	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.	7.5	More Details
CVE-2022-24164	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.	7.5	More Details
CVE-2022-24163	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.	7.5	More Details
CVE-2022-24162	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.	7.5	More Details
CVE-2022-24161	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.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24160	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.	7.5	More Details
CVE-2022-24159	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.	7.5	More Details
CVE-2022-24158	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.	7.5	More Details
CVE-2022-24157	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.	7.5	More Details
CVE-2022-24156	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.	7.5	More Details
CVE-2022-24155	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.	7.5	More Details
CVE-2022-24154	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.	7.5	More Details
CVE-2022-24153	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.	7.5	More Details
CVE-2022-24152	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.	7.5	More Details
CVE-2022-24151	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.	7.5	More Details
CVE-2022-0481	NULL Pointer Dereference in Homebrew mruby prior to 3.2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24147	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.	7.5	More Details
CVE-2022-24143	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.	7.5	More Details
CVE-2021-45997	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.	7.5	More Details
CVE-2021-45737	TOTOLINK A720R v4.1.5cu.470_B20200911 was discovered to contain a stack overflow in the Form_Login function. This vulnerability allows attackers to cause a Denial of Service (DoS) via the Host parameter.	7.5	More Details
CVE-2021-46320	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.	7.5	More Details
CVE-2022-23913	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.	7.5	More Details
CVE-2021-23507	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. *Note:* This vulnerability derives from an incomplete fix in https://security.snyk.io/vuln/SNYK-JS-OBJECTPATHSET-607908	7.5	More Details
CVE-2021-23497	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	7.5	More Details
CVE-2021-45739	TOTOLINK A720R v4.1.5cu.470_B20200911 was discovered to contain a stack overflow in the Form_Login function. This vulnerability allows attackers to cause a Denial of Service (DoS) via the flag parameter.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45741	TOTOLINK X5000R v9.1.0u.6118_B20201102 was discovered to contain a stack overflow in the function setIpv6Cfg. This vulnerability allows attackers to cause a Denial of Service (DoS) via the relay6to4 parameters.	7.5	More Details
CVE-2021-45988	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.	7.5	More Details
CVE-2021-45989	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.	7.5	More Details
CVE-2021-29397	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.	7.5	More Details
CVE-2021-29395	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.	7.5	More Details
CVE-2022-24149	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.	7.5	More Details
CVE-2021-45991	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.	7.5	More Details
CVE-2021-45992	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.	7.5	More Details
CVE-2021-45993	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.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44977	In iCMS <=8.0.0, a directory traversal vulnerability allows an attacker to read arbitrary files.	7.5	More Details
CVE-2021-45994	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.	7.5	More Details
CVE-2021-45995	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.	7.5	More Details
CVE-2022-21712	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.	7.5	More Details
CVE-2021-45996	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.	7.5	More Details
CVE-2021-28503	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.	7.4	More Details
CVE-2021-21964	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.	7.4	More Details
CVE-2021-44205	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	7.3	More Details
CVE-2021-44206	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	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44779	Unauthenticated SQL Injection (SQLi) vulnerability discovered in [GWA] AutoResponder WordPress plugin (versions <= 2.3), vulnerable at (&listid). No patched version available, plugin closed.	7.3	More Details
CVE-2021-25095	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.	7.1	More Details
CVE-2022-0522	Access of Memory Location Before Start of Buffer in NPM radare2.js prior to 5.6.2.	7.1	More Details
CVE-2022-0518	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.6.2.	7.1	More Details
CVE-2022-0519	Buffer Access with Incorrect Length Value in GitHub repository radareorg/radare2 prior to 5.6.2.	7.1	More Details
CVE-2021-25108	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.	7.1	More Details
CVE-2022-0521	Access of Memory Location After End of Buffer in GitHub repository radareorg/radare2 prior to 5.6.2.	7.1	More Details
CVE-2022-23805	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.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23563	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.	7.1	More Details
CVE-2022-21724	pgjdbc is the offical PostgreSQL JDBC Driver. A security hole was found in the jdbc driver for postgresql database while doing security research. The system using the postgresql library will be attacked when attacker control the jdbc url or properties. pgjdbc instantiates plugin instances based on class names provided via `authenticationPluginClassName`, `sslhostnameverifier`, `socketFactory`, `sslfactory`, `sslpasswordcallback` connection properties. However, the driver did not verify if the class implements the expected interface before instantiating the class. This can lead to code execution loaded via arbitrary classes. Users using plugins are advised to upgrade. There are no known workarounds for this issue.	7.0	More Details
CVE-2022-24114	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	7.0	More Details
CVE-2021-42059	An issue was discovered in Insyde InsydeH2O Kernel 5.0 before 05.08.41, Kernel 5.1 before 05.16.41, Kernel 5.2 before 05.26.41, Kernel 5.3 before 05.35.41, and Kernel 5.4 before 05.42.20. A stack-based buffer overflow leads toarbitrary code execution in UEFI DisplayTypeDxe DXE driver.	6.7	More Details
CVE-2021-29218	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.	6.7	More Details
CVE-2021-36193	Multiple stack-based buffer overflows in the command line interpreter of FortiWeb before 6.4.2 may allow an authenticated attacker to achieve arbitrary code execution via specially crafted commands.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21702	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.	6.5	More Details
CVE-2022-23588	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.	6.5	More Details
CVE-2022-23586	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 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23589	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.	6.5	More Details
CVE-2022-23583	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.	6.5	More Details
CVE-2021-44864	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.	6.5	More Details
CVE-2021-44957	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.	6.5	More Details
CVE-2021-44956	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.	6.5	More Details
CVE-2022-0505	Cross-Site Request Forgery (CSRF) in Packagist microweber/microweber prior to 1.2.11.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0504	Generation of Error Message Containing Sensitive Information in Packagist microweber/microweber prior to 1.2.11.	6.5	More Details
CVE-2022-23581	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.	6.5	More Details
CVE-2021-25096	The IP2Location Country Blocker WordPress plugin before 2.26.5 bans can be bypassed by using a specific parameter in the URL	6.5	More Details
CVE-2021-24993	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	6.5	More Details
CVE-2021-24947	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	6.5	More Details
CVE-2021-24928	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.	6.5	More Details
CVE-2021-24843	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.	6.5	More Details
CVE-2022-22679	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.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43929	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.	6.5	More Details
CVE-2022-23582	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.	6.5	More Details
CVE-2022-24301	In Minetest before 5.4.0, players can add or subtract items from a different player's inventory.	6.5	More Details
CVE-2022-23580	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.	6.5	More Details
CVE-2022-23557	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.	6.5	More Details
CVE-2022-23569	Tensorflow is an Open Source Machine Learning Framework. Multiple operations in TensorFlow can be used to trigger a denial of service via `CHECK`-fails (i.e., assertion failures). This is similar to TFSA-2021-198 and has similar fixes. We have patched the reported issues in multiple GitHub commits. It is possible that other similar instances exist in TensorFlow, we will issue fixes as these are discovered. 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.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21737	Tensorflow is an Open Source Machine Learning Framework. The implementation of `*Bincount` operations allows malicious users to cause denial of service by passing in arguments which would trigger a `CHECK`-fail. There are several conditions that the input arguments must satisfy. Some are not caught during shape inference and others are not caught during kernel implementation. This results in `CHECK` failures later when the output tensors get allocated. 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.	6.5	More Details
CVE-2022-21738	Tensorflow is an Open Source Machine Learning Framework. The implementation of `SparseCountSparseOutput` can be made to crash a TensorFlow process by an integer overflow whose result is then used in a memory allocation. 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.	6.5	More Details
CVE-2022-21739	Tensorflow is an Open Source Machine Learning Framework. The implementation of `QuantizedMaxPool` has an undefined behavior where user controlled inputs can trigger a reference binding to 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.	6.5	More Details
CVE-2022-21741	Tensorflow is an Open Source Machine Learning Framework. ### Impact An attacker can craft a TFLite model that would trigger a division by zero in the implementation of depthwise convolutions. The parameters of the convolution can be user controlled and are also used within a division operation to determine the size of the padding that needs to be added before applying the convolution. There is no check before this division that the divisor is strictly positive. 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.	6.5	More Details
CVE-2021-29394	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.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21729	Tensorflow is an Open Source Machine Learning Framework. The implementation of `UnravelIndex` is vulnerable to a division by zero caused by an integer overflow bug. 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.	6.5	More Details
CVE-2022-23579	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.	6.5	More Details
CVE-2022-21725	Tensorflow is an Open Source Machine Learning Framework. The estimator for the cost of some convolution operations can be made to execute a division by 0. The function fails to check that the stride argument is strictly positive. Hence, the fix is to add a check for the stride argument to ensure it is valid. 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.	6.5	More Details
CVE-2022-23568	Tensorflow is an Open Source Machine Learning Framework. The implementation of `AddManySparseToTensorsMap` is vulnerable to an integer overflow which results in a `CHECK`-fail when building new `TensorShape` objects (so, an assert failure based denial of service). We are missing some validation on the shapes of the input tensors as well as directly constructing a large `TensorShape` with user-provided dimensions. 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.	6.5	More Details
CVE-2022-23567	Tensorflow is an Open Source Machine Learning Framework. The implementations of `Sparse*Cwise*` ops are vulnerable to integer overflows. These can be used to trigger large allocations (so, OOM based denial of service) or `CHECK`-fails when building new `TensorShape` objects (so, assert failures based denial of service). We are missing some validation on the shapes of the input tensors as well as directly constructing a large `TensorShape` with user-provided dimensions. 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.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21734	Tensorflow is an Open Source Machine Learning Framework. The implementation of `MapStage` is vulnerable a `CHECK`-fail if the key tensor is not a scalar. 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.	6.5	More Details
CVE-2022-21731	Tensorflow is an Open Source Machine Learning Framework. The implementation of shape inference for `ConcatV2` can be used to trigger a denial of service attack via a segfault caused by a type confusion. The `axis` argument is translated into `concat_dim` in the `ConcatShapeHelper` helper function. Then, a value for `min_rank` is computed based on `concat_dim`. This is then used to validate that the `values` tensor has at least the required rank. However, `WithRankAtLeast` receives the lower bound as a 64-bits value and then compares it against the maximum 32-bits integer value that could be represented. Due to the fact that `min_rank` is a 32-bits value and the value of `axis`, the `rank` argument is a negative value, so the error check is bypassed. 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.	6.5	More Details
CVE-2022-22726	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)	6.5	More Details
CVE-2021-38130	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.	6.5	More Details
CVE-2022-23564	Tensorflow is an Open Source Machine Learning Framework. When decoding a resource handle tensor from protobuf, a TensorFlow process can encounter cases 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.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23570	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.	6.5	More Details
CVE-2022-23577	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.	6.5	More Details
CVE-2022-23576	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.	6.5	More Details
CVE-2022-23575	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.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23572	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.	6.5	More Details
CVE-2022-23571	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.	6.5	More Details
CVE-2022-23565	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.	6.5	More Details
CVE-2022-21735	Tensorflow is an Open Source Machine Learning Framework. The implementation of `FractionalMaxPool` can be made to crash a TensorFlow process via a division by 0. 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.	6.5	More Details
CVE-2021-40403	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.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21703	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.	6.3	More Details
CVE-2022-23262	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	6.3	More Details
CVE-2022-21814	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.	6.1	More Details
CVE-2022-0380	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.	6.1	More Details
CVE-2022-0149	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.	6.1	More Details
CVE-2022-22146	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.	6.1	More Details
CVE-2022-21813	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.	6.1	More Details
CVE-2021-43635	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.	6.1	More Details
CVE-2021-24878	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	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45281	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.	6.1	More Details
CVE-2022-22142	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.	6.1	More Details
CVE-2022-21805	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.	6.1	More Details
CVE-2021-43062	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiMail version 7.0.1 and 7.0.0, version 6.4.5 and below, version 6.3.7 and below, version 6.0.11 and below allows attacker to execute unauthorized code or commands via crafted HTTP GET requests to the FortiGuard URI protection service.	6.1	More Details
CVE-2021-45329	Cross Site Scripting (XSS) vulnerability exists in Gitea before 1.5.1 via the repository settings inside the external wiki/issue tracker URL field.	6.1	More Details
CVE-2021-45408	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.	6.1	More Details
CVE-2022-0381	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.	6.1	More Details
CVE-2021-25077	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	6.1	More Details
CVE-2022-0437	Cross-site Scripting (XSS) - DOM in NPM karma prior to 6.3.14.	6.1	More Details
CVE-2022-0432	Prototype Pollution in GitHub repository mastodon/mastodon prior to 3.5.0.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42639	PrinterLogic Web Stack versions 19.1.1.13 SP9 and below are vulnerable to multiple reflected cross site scripting vulnerabilities. Attacker controlled input is reflected back in the page without sanitization.	6.1	More Details
CVE-2022-0501	Cross-site Scripting (XSS) - Reflected in Packagist ptrofimov/beanstalk_console prior to 1.7.12.	6.1	More Details
CVE-2022-23184	In affected Octopus Server versions when the server HTTP and HTTPS bindings are configured to localhost, Octopus Server will allow open redirects.	6.1	More Details
CVE-2022-22818	The {% debug %} template tag in Django 2.2 before 2.2.27, 3.2 before 3.2.12, and 4.0 before 4.0.2 does not properly encode the current context. This may lead to XSS.	6.1	More Details
CVE-2021-45328	Gitea before 1.4.3 is affected by URL Redirection to Untrusted Site ('Open Redirect') via internal URLs.	6.1	More Details
CVE-2022-23593	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.	5.9	More Details
CVE-2022-23590	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.	5.9	More Details
CVE-2021-21963	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.	5.9	More Details
CVE-2021-21971	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.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-36151	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.	5.5	More Details
CVE-2022-21815	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.	5.5	More Details
CVE-2022-21816	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.	5.5	More Details
CVE-2021-4043	NULL Pointer Dereference in GitHub repository gpac/gpac prior to 1.1.0.	5.5	More Details
CVE-2022-0264	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	5.5	More Details
CVE-2020-12966	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.	5.5	More Details
CVE-2021-45429	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.	5.5	More Details
CVE-2022-0487	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.	5.5	More Details
CVE-2022-24249	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.	5.5	More Details
CVE-2021-45919	Studio 42 elFinder through 2.1.31 allows XSS via an SVG document.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0506	Cross-site Scripting (XSS) - Stored in Packagist microweber/microweber prior to 1.2.11.	5.4	More Details
CVE-2022-0502	Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.	5.4	More Details
CVE-2022-22804	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)	5.4	More Details
CVE-2022-0510	Cross-site Scripting (XSS) - Reflected in Packagist pimcore/pimcore prior to 10.3.1.	5.4	More Details
CVE-2022-23871	Multiple cross-site scripting (XSS) vulnerabilities in the component outcomes_addProcess.php of Gibbon CMS v22.0.01 allow attackers to execute arbitrary web scripts or HTML via a crafted payload insterted into the name, category, description parameters.	5.4	More Details
CVE-2021-43841	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.	5.4	More Details
CVE-2021-32036	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. This issue affects MongoDB Server v5.0 versions prior to and including 5.0.3; MongoDB Server v4.4 versions prior to and including 4.4.9; MongoDB Server v4.2 versions prior to and including 4.2.16 and MongoDB Server v4.0 versions prior to and including 4.0.28	5.4	More Details
CVE-2022-0148	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.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24880	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	5.4	More Details
CVE-2021-25106	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	5.4	More Details
CVE-2022-0509	Cross-site Scripting (XSS) - Stored in Packagist pimcore/pimcore prior to 10.3.1.	5.4	More Details
CVE-2022-0472	Unrestricted Upload of File with Dangerous Type in Packagist jsdecena/laracom prior to v2.0.9.	5.4	More Details
CVE-2022-0508	Server-Side Request Forgery (SSRF) in GitHub repository chocobozzz/peertube prior to f33e515991a32885622b217bf2ed1d1b0d9d6832	5.3	More Details
CVE-2021-46671	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.	5.3	More Details
CVE-2020-26208	JHEAD is a simple command line tool for displaying and some manipulation of EXIF header data embedded in Jpeg images from digital cameras. In affected versions there is a heap-buffer-overflow on jhead-3.04/jpgfile.c:285 ReadJpegSections. Crafted jpeg images can be provided to the user resulting in a program crash or potentially incorrect exif information retrieval. Users are advised to upgrade. There is no known workaround for this issue.	5.3	More Details
CVE-2021-42633	PrinterLogic Web Stack versions 19.1.1.13 SP9 and below are vulnerable to SQL Injection, which may allow an attacker to access additional audit records.	5.3	More Details
CVE-2022-23261	Microsoft Edge (Chromium-based) Tampering Vulnerability	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-39021	IBM Guardium Data Encryption (GDE) 5.0.0.2 behaves differently or sends different responses under different circumstances in a way that is observable to an unauthorized actor, which could facilitate username enumeration. IBM X-Force ID: 213856.	5.3	More Details
CVE-2021-44886	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.	5.3	More Details
CVE-2021-29398	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.	5.3	More Details
CVE-2022-23595	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.	5.3	More Details
CVE-2022-22680	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.	5.3	More Details
CVE-2022-23600	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.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21799	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.	5.2	More Details
CVE-2022-23627	ArchiSteamFarm (ASF) is a C# application with primary purpose of idling Steam cards from multiple accounts simultaneously. Due to a bug in ASF code, introduced in version V5.2.2.2, the program didn't adequately verify effective access of the user sending proxy (i.e. `[Bots]`) commands. In particular, a proxy-like command sent to bot `A` targeting bot `B` has incorrectly verified user's access against bot `A` - instead of bot `B`, to which the command was originally designated. This in result allowed access to resources beyond those configured, being a security threat affecting confidentiality of other bot instances. A successful attack exploiting this bug requires a significant access granted explicitly by original owner of the ASF process prior to that, as attacker has to control at least a single bot in the process to make use of this inadequate access verification loophole. The issue is patched in ASF V5.2.2.5, V5.2.3.2 and future versions. Users are advised to update as soon as possible.	5.0	More Details
CVE-2022-23316	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.	4.9	More Details
CVE-2021-44983	In taocms 3.0.1 after logging in to the background, there is an Arbitrary file download vulnerability at the File Management column.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22939	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.	4.9	More Details
CVE-2021-25004	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.	4.9	More Details
CVE-2021-20877	Cross-site scripting vulnerability in Canon laser printers and small office multifunctional printers (LBP162L/LBP162, MF4890dw, MF269dw/MF265dw/MF264dw/MF262dw, MF249dw/MF245dw/MF244dw/MF242dw/MF232w, and MF229dw/MF224dw/MF222dw sold in Japan, imageCLASS MF Series (MF113W/MF212W/MF217W/MF227DW/MF229DW, MF232W/MF244DW/MF247DW/MF249DW, MF264DW/MF267DW/MF269DW/MF269DW VP, and MF4570DN/MF4570DW/MF4770N/MF4880DW/MF4890DW) and imageCLASS LBP Series (LBP113W/LBP151DW/LBP162DW) sold in the US, and iSENSYS (LBP162DW, LBP113W, LBP151DW, MF269dw, MF267dw, MF264dw, MF113w, MF249dw, MF247dw, MF244dw, MF237w, MF232w, MF229dw, MF217w, MF212w, MF4780w, and MF4890dw) and imageRUNNER (2206IF, 2204N, and 2204F) sold in Europe) allows remote attackers to inject an arbitrary script via unspecified vectors.	4.8	More Details
CVE-2021-25105	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.	4.8	More Details
CVE-2021-25029	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	4.8	More Details
CVE-2022-23980	Cross-Site Scripting (XSS) vulnerability discovered in Yasr – Yet Another Stars Rating WordPress plugin (versions <= 2.9.9), vulnerable at parameter 'source'.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43925	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.	4.7	More Details
CVE-2021-43926	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.	4.7	More Details
CVE-2021-43927	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.	4.7	More Details
CVE-2021-25103	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	4.7	More Details
CVE-2022-23605	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.	4.4	More Details
CVE-2022-21732	Tensorflow is an Open Source Machine Learning Framework. The implementation of `ThreadPoolHandle` can be used to trigger a denial of service attack by allocating too much memory. This is because the `num_threads` argument is only checked to not be negative, but there is no upper bound on its value. 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.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21733	Tensorflow is an Open Source Machine Learning Framework. The implementation of `StringNGrams` can be used to trigger a denial of service attack by causing an out of memory condition after an integer overflow. We are missing a validation on `pad_witdh` and that result in computing a negative value for `ngram_width` which is later used to allocate parts of the output. 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.	4.3	More Details
CVE-2022-21713	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 ID. Users are advised to upgrade as soon as possible. There are no known workarounds for this issue.	4.3	More Details
CVE-2022-22931	Fix of CVE-2021-40525 do not prepend delimiters upon valid directory validations. Affected implementations include: - maildir mailbox store - Sieve file repository This enables a user to access other users data stores (limited to user names being prefixed by the value of the username being used).	4.3	More Details
CVE-2022-23585	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.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23578	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.	4.3	More Details
CVE-2021-25084	The Advanced Cron Manager WordPress plugin before 2.4.2 and Advanced Cron Manager Pro WordPress plugin before 2.5.3 do not have authorisation checks in some of their AJAX actions, allowing any authenticated users, such as subscriber to call them and add or remove events as well as schedules for example	4.3	More Details
CVE-2021-36177	An improper access control vulnerability [CWE-284] in FortiAuthenticator HA service 6.3.2 and below, 6.2.x, 6.1.x, 6.0.x may allow an attacker on the same vlan as the HA management interface to make an unauthenticated direct connection to the FAC's database.	4.2	More Details
CVE-2022-0317	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.	4.0	More Details
CVE-2022-0473	OTRS administrators can configure dynamic field and inject malicious JavaScript code in the error message of the regular expression check. When used in the agent interface, malicious code might be exectued in the browser. This issue affects: OTRS AG OTRS 7.0.x version: 7.0.31 and prior versions.	3.8	More Details
CVE-2022-24448	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.	3.3	More Details
CVE-2022-0474	Full list of recipients from customer users in a contact field could be disclosed in notification emails event when the notification is set to be sent to each recipient individually. This issue affects: OTRS AG OTRSCustomContactFields 8.0.x version: 8.0.11 and prior versions.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0227	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-0498	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details