SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 18 August 2021

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	Refere
CVE-2021-37705	OneFuzz is an open source self-hosted Fuzzing-As-A-Service platform. Starting with OneFuzz 2.12.0 or greater, an incomplete authorization check allows an authenticated user from any Azure Active Directory tenant to make authorized API calls to a vulnerable OneFuzz instance. To be vulnerable, a OneFuzz deployment must be both version 2.12.0 or greater and deployed with the non-default --multi_tenant_domain option. This can result in read/write access to private data such as software vulnerability and crash information, security testing tools and proprietary code and symbols. Via authorized API calls, this also enables tampering with existing data and unauthorized code execution on Azure compute resources. This issue is resolved starting in release 2.31.0, via the addition of application-level check of the bearer token's `issuer` against an administrator-configured allowlist. As a workaround users can restrict access to the tenant of a deployed OneFuzz instance < 2.31.0 by redeploying in the default configuration, which omits the `--multi_tenant_domain` option.	10.0	More Details
CVE-2021-38516	Certain NETGEAR devices are affected by lack of access control at the function level. This affects D6220 before 1.0.0.48, D6400 before 1.0.0.82, D7000v2 before 1.0.0.52, D7800 before 1.0.1.44, D8500 before 1.0.3.43, DC112A before 1.0.0.40, DGN2200v4 before 1.0.0.108, RBK50 before 2.3.0.32, RBR50 before 2.3.0.32, RBS50 before 2.3.0.32, RBK20 before 2.3.0.28, RBR20 before 2.3.0.28, RBS20 before 2.3.0.28, RBK40 before 2.3.0.28, RBR40 before 2.3.0.28, RBS40 before 2.3.0.28, R6020 before 1.0.0.34, R6080 before 1.0.0.34, R6120 before 1.0.0.44, R6220 before 1.1.0.80, R6230 before 1.1.0.80, R6250 before 1.0.4.34, R6260 before 1.1.0.40, R6850 before 1.1.0.40, R6350 before 1.1.0.40, R6400v2 before 1.0.2.62, R6700v3 before 1.0.2.62, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900v2 before 1.2.0.36, R7000 before 1.0.9.34, R6900P before 1.3.1.44, R7000P before 1.3.1.44, R7100LG before 1.0.0.48, R7200 before 1.2.0.48, R7350 before 1.2.0.48, R7400 before 1.2.0.48, R7450 before 1.2.0.36, AC2100 before 1.2.0.36, AC2400 before 1.2.0.36, AC2600 before 1.2.0.36, R7500v2 before 1.0.3.38, R7800 before 1.0.2.58, R7900 before 1.0.3.8, R7960P before 1.4.1.44, R8000 before 1.0.4.28, R7900P before 1.4.1.30, R8000P before 1.4.1.30, R8900 before 1.0.4.2, R9000 before 1.0.4.2, RAX120 before 1.0.0.74, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 before 3.2.16.6, RBR850 before 3.2.16.6, RBS850 before 3.2.16.6, WNR3500Lv2 before 1.2.0.56, XR450 before 2.3.2.32, and XR500 before 2.3.2.32.	10.0	More Details
CVE-2021-26424	Windows TCP/IP Remote Code Execution Vulnerability	9.9	More Details
CVE-2021-36380	Sunhillo SureLine before 8.7.0.1.1 allows Unauthenticated OS Command Injection via shell metacharacters in ipAddr or dnsAddr /cgi/networkDiag.cgi.	9.8	More Details
CVE-2021-21830	A heap-based buffer overflow vulnerability exists in the XML Decompression LabelDict::Load functionality of AT&T Labs' Xmill 0.7. A specially crafted XMI file can lead to remote code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2021-21829	A heap-based buffer overflow vulnerability exists in the XML Decompression EnumerationUncompressor::UncompressItem functionality of AT&T Labs' Xmill 0.7. A specially crafted XMI file can lead to remote code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2021-38302	The Newsletter extension through 4.0.0 for TYPO3 allows SQL Injection.	9.8	More Details
CVE-2021-36789	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 allows SQL Injection.	9.8	More Details
CVE-2020-18758	An issue in Dut Computer Control Engineering Co.'s PLC MAC1100 allows attackers to execute arbitrary code.	9.8	More Details

CVE Number	Description	Base Score	Refere
CVE-2020-18753	An issue in Dut Computer Control Engineering Co.'s PLC MAC1100 allows attackers to gain access to the system and escalate privileges via a crafted packet.	9.8	More Details
CVE-2021-32122	Certain NETGEAR devices are affected by CSRF. This affects EX3700 before 1.0.0.90, EX3800 before 1.0.0.90, EX6120 before 1.0.0.64, and EX6130 before 1.0.0.44.	9.8	More Details
CVE-2021-24527	The User Registration & User Profile – Profile Builder WordPress plugin before 3.4.9 has a bug allowing any user to reset the password of the admin of the blog, and gain unauthorised access, due to a bypass in the way the reset key is checked. Furthermore, the admin will not be notified of such change by email for example.	9.8	More Details
CVE-2021-1104	The RISC-V Instruction Set Manual contains a documented ambiguity for the Machine Trap Vector Base Address (MTVEC) register that may lead to a vulnerability due to the initial state of the register not being defined, potentially leading to information disclosure, data tampering and denial of service.	9.8	More Details
CVE-2021-37353	Nagios XI Docker Wizard before version 1.1.3 is vulnerable to SSRF due to improper sanitation in table_population.php.	9.8	More Details
CVE-2021-37350	Nagios XI before version 5.8.5 is vulnerable to SQL injection vulnerability in Bulk Modifications Tool due to improper input sanitisation.	9.8	More Details
CVE-2021-37346	Nagios XI WatchGuard Wizard before version 1.4.8 is vulnerable to remote code execution through Improper neutralisation of special elements used in an OS Command (OS Command injection).	9.8	More Details
CVE-2021-37344	Nagios XI Switch Wizard before version 2.5.7 is vulnerable to remote code execution through improper neutralisation of special elements used in an OS Command (OS Command injection).	9.8	More Details
CVE-2021-32071	The MiCollab Client service in Mitel MiCollab before 9.3 could allow an unauthenticated user to gain system access due to improper access control. A successful exploit could allow an attacker to view and modify application data, and cause a denial of service for users.	9.8	More Details
CVE-2021-35393	Realtek Jungle SDK version v2.x up to v3.4.14B provides a 'WiFi Simple Config' server that implements both UPnP and SSDP protocols. The binary is usually named wscd or mini_upnpd and is the successor to miniigd. The server is vulnerable to a stack buffer overflow vulnerability that is present due to unsafe parsing of the UPnP SUBSCRIBE/UNSUBSCRIBE Callback header. Successful exploitation of this vulnerability allows remote unauthenticated attackers to gain arbitrary code execution on the affected device.	9.8	More Details
CVE-2021-31556	An issue was discovered in the Oauth extension for MediaWiki through 1.35.2. MWOAuthConsumerSubmitControl.php does not ensure that the length of an RSA key will fit in a MySQL blob.	9.8	More Details
CVE-2021-35394	Realtek Jungle SDK version v2.x up to v3.4.14B provides a diagnostic tool called 'MP Daemon' that is usually compiled as 'UDPServer' binary. The binary is affected by multiple memory corruption vulnerabilities and an arbitrary command injection vulnerability that can be exploited by remote unauthenticated attackers.	9.8	More Details
CVE-2021-35395	Realtek Jungle SDK version v2.x up to v3.4.14B provides an HTTP web server exposing a management interface that can be used to configure the access point. Two versions of this management interface exists: one based on Go-Ahead named webs and another based on Boa named boa. Both of them are affected by these vulnerabilities. Specifically, these binaries are vulnerable to the following issues: - stack buffer overflow in formRebootCheck due to unsafe copy of submit-url parameter - stack buffer overflow in formWsc due to unsafe copy of submit-url parameter - stack buffer overflow in formWlanMultipleAP due to unsafe copy of submit-url parameter - stack buffer overflow in formWlSiteSurvey due to unsafe copy of ifname parameter - stack buffer overflow in formStaticDHCP due to unsafe copy of hostname parameter - stack buffer overflow in formWsc due to unsafe copy of 'peerPin' parameter - arbitrary command execution in formSysCmd via the sysCmd parameter - arbitrary command injection in formWsc via the 'peerPin' parameter Exploitability of identified issues will differ based on what the end vendor/manufacturer did with the Realtek SDK webserver. Some vendors use it as-is, others add their own authentication implementation, some kept all the features from the server, some remove some of them, some inserted their own set of features. However, given that Realtek SDK implementation is full of insecure calls and that developers tends to re-use those examples in their custom code, any binary based on Realtek SDK webserver will probably contains its own set of issues on top of the Realtek ones (if kept). Successful exploitation of these issues allows remote attackers to gain arbitrary code execution on the device.	9.8	More Details
CVE-2021-38753	An unrestricted file upload on Simple Image Gallery Web App can be exploited to upload a web shell and executed to gain unauthorized access to the server hosting the web app.	9.8	More Details
CVE-2021-38754	SQL Injection vulnerability in Hospital Management System due to lack of input validation in messearch.php.	9.8	More Details
CVE-2020-18698	Improper Authentication in Lin-CMS-Flask v0.1.1 allows remote attackers to launch brute force login attempts without restriction via the 'login' function in the component 'app/api/cms/user.py'.	9.8	More Details

CVE Number	Description	Base Score	Refere
CVE-2020-18701	Incorrect Access Control in Lin-CMS-Flask v0.1.1 allows remote attackers to obtain sensitive information and/or gain privileges due to the application not invalidating a user's authentication token upon logout, which allows for replaying packets.	9.8	More Details
CVE-2020-18703	XML External Entities (XXE) in Quokka v0.4.0 allows remote attackers to execute arbitrary code via the component 'quokka/utils/atom.py'.	9.8	More Details
CVE-2020-18704	Unrestricted Upload of File with Dangerous Type in Django-Widgy v0.8.4 allows remote attackers to execute arbitrary code via the 'image' widget in the component 'Change Widgy Page'.	9.8	More Details
CVE-2020-18705	XML External Entities (XXE) in Quokka v0.4.0 allows remote attackers to execute arbitrary code via the component 'quokka/core/content/views.py'.	9.8	More Details
CVE-2021-22931	Node.js before 16.6.0, 14.17.4, and 12.22.4 is vulnerable to Remote Code Execution, XSS, Application crashes due to missing input validation of host names returned by Domain Name Servers in Node.js dns library which can lead to output of wrong hostnames (leading to Domain Hijacking) and injection vulnerabilities in applications using the library.	9.8	More Details
CVE-2020-22937	A remote code execution (RCE) in e/install/index.php of EmpireCMS 7.5 allows attackers to execute arbitrary PHP code via writing malicious code to the install file.	9.8	More Details
CVE-2021-22156	An integer overflow vulnerability in the calloc() function of the C runtime library of affected versions of BlackBerry® QNX Software Development Platform (SDP) version(s) 6.5.0SP1 and earlier, QNX OS for Medical 1.1 and earlier, and QNX OS for Safety 1.0.1 and earlier that could allow an attacker to potentially perform a denial of service or execute arbitrary code.	9.8	More Details
CVE-2020-18164	SQL Injection vulnerability exists in tp-shop 2.x-3.x via the /index.php/home/api/shop fBill parameter.	9.8	More Details
CVE-2021-21810	A memory corruption vulnerability exists in the XML-parsing ParseAttribs functionality of AT&T Labs' Xmill 0.7. A specially crafted XML file can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2021-31698	Quectel EG25-G devices through 202006130814 allow executing arbitrary code remotely by using an AT command to place shell metacharacters in quectel_handle_fumo_cfg input in atfwd_daemon.	9.8	More Details
CVE-2021-21832	A memory corruption vulnerability exists in the ISO Parsing functionality of Disc Soft Ltd Deamon Tools Pro 8.3.0.0767. A specially crafted malformed file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2021-29377	Pear Admin Think through 2.1.2 has an arbitrary file upload vulnerability that allows attackers to execute arbitrary code remotely. A .php file can be uploaded via admin.php/index/upload because app/common/service/UploadService.php mishandles fileExt.	9.8	More Details
CVE-2020-20975	In \lib\admin\action\dataaction.class.php in Gxlcms v1.1, SQL Injection exists via the $filename parameter.	9.8	More Details
CVE-2021-20418	IBM Security Guardium 11.2 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 196279.	9.8	More Details
CVE-2021-33793	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 have an out-of-bounds write because the Cross-Reference table is mishandled during Office document conversion.	9.8	More Details
CVE-2020-21359	An arbitrary file upload vulnerability in the Template Upload function of Maccms10 allows attackers bypass the suffix whitelist verification to execute arbitrary code via adding a character to the end of the uploaded file's name.	9.8	More Details
CVE-2020-25560	In SapphireIMS 5.0, it is possible to use the hardcoded credential in clients (username: sapphire, password: ims) and gain access to the portal. Once the access is available, the attacker can inject malicious OS commands on "ping", "traceroute" and "snmp" functions and execute code on the server. We also observed the same is true if the JSESSIONID is completely removed.	9.8	More Details
CVE-2020-25563	In SapphireIMS 5.0, it is possible to create local administrator on any client without requiring any credentials by directly accessing RemoteMgmtTaskSave (Automation Tasks) feature and not having a JSESSIONID.	9.8	More Details
CVE-2020-25565	In SapphireIMS 5.0, it is possible to use the hardcoded credential in clients (username: sapphire, password: ims) and gain access to the portal. Once the access is available, the attacker can inject malicious OS commands on "ping", "traceroute" and "snmp" functions and execute code on the server.	9.8	More Details

CVE Number	Description	Base Score	Refere
CVE-2020-25566	In SapphireIMS 5.0, it is possible to take over an account by sending a request to the Save_Password form as shown in POC. Notice that we do not require a JSESSIONID in this request and can reset any user's password by changing the username to that user and password to base64(desired password).	9.8	More Details
CVE-2021-38563	An issue was discovered in Foxit PDF Reader before 11.0.1 and PDF Editor before 11.0.1. It mishandles situations in which an array size (derived from a /Size entry) is smaller than the maximum indirect object number, and thus there is an attempted incorrect array access (leading to a NULL pointer dereference, or out-of-bounds read or write).	9.8	More Details
CVE-2021-38568	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows memory corruption during conversion of a PDF document to a different document format.	9.8	More Details
CVE-2021-38572	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows writing to arbitrary files because the extractPages pathname is not validated.	9.8	More Details
CVE-2021-28890	J2eeFAST 2.2.1 allows remote attackers to perform SQL injection via the (1) compId parameter to fast/sys/user/list, (2) deptId parameter to fast/sys/role/list, or (3) roleId parameter to fast/sys/role/authUser/list, related to the use of ${} to join SQL statements.	9.8	More Details
CVE-2021-38574	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows SQL Injection via crafted data at the end of a string.	9.8	More Details
CVE-2021-37222	Parsers in the open source project RCDCAP before 1.0.5 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via specially crafted packets.	9.8	More Details
CVE-2020-28165	The EasyCorp ZenTao PMS 12.4.2 application suffers from an arbitrary file upload vulnerability. An attacker can upload arbitrary webshell to the server by using the downloadZipPackage() function.	9.8	More Details
CVE-2021-38573	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows writing to arbitrary files because a CombineFiles pathname is not validated.	9.8	More Details
CVE-2021-33199	In Expression Engine before 6.0.3, addonIcon in Addons/file/mod.file.php relies on the untrusted input value of input->get('file') instead of the fixed file names of icon.png and icon.svg.	9.8	More Details
CVE-2020-36363	Amazon AWS CloudFront TLSv1.2_2019 allows TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 and TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, which some entities consider to be weak ciphers.	9.8	More Details
CVE-2021-20314	Stack buffer overflow in libspf2 versions below 1.2.11 when processing certain SPF macros can lead to Denial of service and potentially code execution via malicious crafted SPF explanation messages.	9.8	More Details
CVE-2021-20509	IBM Maximo Asset Management 7.6.0 and 7.6.1 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 198243.	9.8	More Details
CVE-2021-38606	reNgine through 0.5 relies on a predictable directory name.	9.8	More Details
CVE-2021-26432	Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-28121	Virtual Robots.txt before 1.10 does not block HTML tags in the robots.txt field.	9.8	More Details
CVE-2020-20979	An arbitrary file upload vulnerability in the move_uploaded_file() function of LJCMS v4.3 allows attackers to execute arbitrary code.	9.8	More Details
CVE-2021-37599	The exporter/Login.aspx login form in the Exporter in Nuance Winscribe Dictation 4.1.0.99 is vulnerable to SQL injection that allows a remote, unauthenticated attacker to read the database (and execute code in some situations) via the txtPassword parameter.	9.8	More Details
CVE-2021-38528	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D8500 before 1.0.3.58, R6900P before 1.3.2.132, R7000P before 1.3.2.132, R7100LG before 1.0.0.64, WNDR3400v3 before 1.0.1.38, and XR300 before 1.0.3.56.	9.6	More Details

CVE Number	Description	Base Score	Refere
CVE-2021-38530	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects RBK40 before 2.5.1.16, RBR40 before 2.5.1.16, RBS40 before 2.5.1.16, RBK20 before 2.5.1.16, RBR20 before 2.5.1.16, RBS20 before 2.5.1.16, RBK50 before 2.5.1.16, RBR50 before 2.5.1.16, RBS50 before 2.5.1.16, and RBS50Y before 2.6.1.40.	9.6	More Details
CVE-2021-38513	Certain NETGEAR devices are affected by authentication bypass. This affects RBK852 before 3.2.10.11, RBR850 before 3.2.10.11, RBS850 before 3.2.10.11, CBR40 before 2.5.0.10, EAX20 before 1.0.0.48, MK62 before 1.0.6.110, MR60 before 1.0.6.110, MS60 before 1.0.6.110, RBK752 before 3.2.10.10, RBR750 before 3.2.10.10, and RBS750 before 3.2.10.10.	9.6	More Details
CVE-2021-32829	ZStack is open source IaaS(infrastructure as a service) software aiming to automate datacenters, managing resources of compute, storage, and networking all by APIs. Affected versions of ZStack REST API are vulnerable to post-authentication Remote Code Execution (RCE) via bypass of the Groovy shell sandbox. The REST API exposes the GET zstack/v1/batch-queries?script endpoint which is backed up by the BatchQueryAction class. Messages are represented by the APIBatchQueryMsg, dispatched to the QueryFacadeImpl facade and handled by the BatchQuery class. The HTTP request parameter script is mapped to the APIBatchQueryMsg.script property and evaluated as a Groovy script in BatchQuery.query the evaluation of the user-controlled Groovy script is sandboxed by SandboxTransformer which will apply the restrictions defined in the registered (sandbox.register()) GroovyInterceptor. Even though the sandbox heavily restricts the receiver types to a small set of allowed types, the sandbox is non effective at controlling any code placed in Java annotations and therefore vulnerable to meta-programming escapes. This issue leads to post-authenticated remote code execution. For more details see the referenced GHSL-2021-065. This issue is patched in versions 3.8.21, 3.10.8, and 4.1.0.	9.6	More Details
CVE-2021-3616	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow an unauthorized user to view device information, alter firmware content and device configuration. This vulnerability is the same as CNVD-2020-68651.	9.4	More Details
CVE-2021-37678	TensorFlow is an end-to-end open source platform for machine learning. In affected versions TensorFlow and Keras can be tricked to perform arbitrary code execution when deserializing a Keras model from YAML format. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/python/keras/saving/model_config.py#L66-L104) uses `yaml.unsafe_load` which can perform arbitrary code execution on the input. Given that YAML format support requires a significant amount of work, we have removed it for now. We have patched the issue in GitHub commit 23d6383eb6c14084a8fc3bdf164043b974818012. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.	9.3	More Details
CVE-2021-33794	Foxit Reader before 10.1.4 and PhantomPDF before 10.1.4 allow information disclosure or an application crash after mishandling the Tab key during XFA form interaction.	9.1	More Details
CVE-2021-27741	" Security vulnerability in HCL Commerce Management Center allowing XML external entity (XXE) injection"	9.1	More Details
CVE-2021-38621	The remove API in v1/controller/cloudStorage/alibabaCloud/remove/index.ts in netless Agora Flat Server before 2021-07-30 mishandles file ownership.	9.1	More Details
CVE-2021-38564	An issue was discovered in Foxit PDF Reader before 11.0.1 and PDF Editor before 11.0.1. It allows an out-of-bounds read via util.scand.	9.1	More Details
CVE-2021-38570	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows attackers to delete arbitrary files (during uninstallation) via a symlink.	9.1	More Details
CVE-2019-25052	In Linaro OP-TEE before 3.7.0, by using inconsistent or malformed data, it is possible to call update and final cryptographic functions directly, causing a crash that could leak sensitive information.	9.1	More Details
CVE-2021-3352	The Software Development Kit in Mitel MiContact Center Business from 8.0.0.0 through 8.1.4.1 and 9.0.0.0 through 9.3.1.0 could allow an unauthenticated attacker to access (view and modify) user data without authorization due to improper handling of tokens.	9.1	More Details
CVE-2021-34823	The ON24 ScreenShare (aka DesktopScreenShare.app) plugin before 2.0 for macOS allows remote file access via its built-in HTTP server. This allows unauthenticated remote users to retrieve files accessible to the logged-on macOS user. When a remote user sends a crafted HTTP request to the server, it triggers a code path that will download a configuration file from a specified remote machine over HTTP. There is an XXE flaw in processing of this configuration file that allows reading local (to macOS) files and uploading them to remote machines.	9.1	More Details
CVE-2021-25955	In “Dolibarr ERP CRM”, WYSIWYG Editor module, v2.8.1 to v13.0.2 are affected by a stored XSS vulnerability that allows low privileged application users to store malicious scripts in the “Private Note” field at “/adherents/note.php?id=1” endpoint. These scripts are executed in a victim’s browser when they open the page containing the vulnerable field. In the worst case, the victim who inadvertently triggers the attack is a highly privileged administrator. The injected scripts can extract the Session ID, which can lead to full Account takeover of the admin and due to other vulnerability (Improper Access Control on Private notes) a low privileged user can update the private notes which could lead to privilege escalation.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description

CVE Number	Description
CVE-2021-21861	An exploitable integer truncation vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. When processir FOURCC code, a specially crafted MPEG-4 input can cause an improper memory allocation resulting in a heap-based buffer overflow that causes memory corruption. A can convince a user to open a video to trigger this vulnerability.
CVE-2021-36921	AIMANAGER before B115 on MONITORAPP Application Insight Web Application Firewall (AIWAF) devices with Manager 2.1.0 has Improper Authentication. An attack administrative access by modifying the response to an authentication check request.
CVE-2021-29988	Firefox incorrectly treated an inline list-item element as a block element, resulting in an out of bounds read or memory corruption, and a potentially exploitable crash. Th vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
CVE-2021-37708	Shopware is an open source eCommerce platform. Versions prior to 6.4.3.1 contain a command injection vulnerability in mail agent settings. Version 6.4.3.1 contains a workarounds for older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin.
CVE-2020-18460	Cross Site Request Forgery (CSRF) vulnerability exists in 711cms v1.0.7 that can add an admin account via admin.php?c=Admin&m=content.
CVE-2021-29989	Mozilla developers reported memory safety bugs present in Firefox 90 and Firefox ESR 78.12. Some of these bugs showed evidence of memory corruption and we pre with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.13, Firefox ESR < 78.13, and Firefox < 91.
CVE-2021-29990	Mozilla developers and community members reported memory safety bugs present in Firefox 90. Some of these bugs showed evidence of memory corruption and we p that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 91.
CVE-2021-21860	An exploitable integer truncation vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. A specially craf 4 input can cause an improper memory allocation resulting in a heap-based buffer overflow that causes memory corruption. The FOURCC code, 'trik', is parsed by the within the library. An attacker can convince a user to open a video to trigger this vulnerability.
CVE-2021-21859	An exploitable integer truncation vulnerability exists within the MPEG-4 decoding functionality of the GPAC Project on Advanced Content library v1.0.1. The stri_box_re is used when processing atoms using the 'stri' FOURCC code. An attacker can convince a user to open a video to trigger this vulnerability.
CVE-2021-29985	A use-after-free vulnerability in media channels could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
CVE-2020-28589	An improper array index validation vulnerability exists in the LoadObj functionality of tinyobjloader v2.0-rc1 and tinyobjloader development commit 79d4421. A specially could lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.
CVE-2021-3050	An OS command injection vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator to execute arbitrary OS commands to e privileges. This issue impacts: PAN-OS 9.0 version 9.0.10 through PAN-OS 9.0.14; PAN-OS 9.1 version 9.1.4 through PAN-OS 9.1.10; PAN-OS 10.0 version 10.0.7 ar PAN-OS 10.0 versions; PAN-OS 10.1 version 10.1.0 through PAN-OS 10.1.1. Prisma Access firewalls and firewalls running PAN-OS 8.1 versions are not impacted by
CVE-2020-21976	An arbitrary file upload in the <input type="file" name="user_image"> component of NewsOne CMS v1.1.0 allows attackers to webshell and execute arbitrary command
CVE-2021-36947	Windows Print Spooler Remote Code Execution Vulnerability
CVE-2020-22403	Cross Site Request Forgery (CSRF) vulnerability in Express cart v1.1.16 allows attackers to add an administrator account, add discount code or other unspecified impa
CVE-2021-29984	Instruction reordering resulted in a sequence of instructions that would cause an object to be incorrectly considered during garbage collection. This led to memory corru a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
CVE-2021-36936	Windows Print Spooler Remote Code Execution Vulnerability
CVE-2021-38366	Sitecore through 10.1, when Update Center is enabled, allows remote authenticated users to upload arbitrary files and achieve remote code execution by visiting an up .aspx file at an admin/Packages URL.
CVE-2021-25957	In “Dolibarr” application, v2.8.1 to v13.0.2 are vulnerable to account takeover via password reset functionality. A low privileged attacker can reset the password of any u application using the password reset link the user received through email when requested for a forgotten password.

CVE Number	Description
CVE-2017-16630	In SapphireIMS 4097_1, a guest user can create a local administrator account on any system that has SapphireIMS installed, because of an Insecure Direct Object Ref (IDOR) in the local user creation function.
CVE-2021-29980	Uninitialized memory in a canvas object could have caused an incorrect free() leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
CVE-2021-34535	Remote Desktop Client Remote Code Execution Vulnerability
CVE-2020-25564	In SapphireIMS 5.0, it is possible to create local administrator on any client with credentials of a non-privileged user by directly accessing RemoteMgmtTaskSave (Auto Tasks) feature.
CVE-2021-29981	An issue present in lowering/register allocation could have led to obscure but deterministic register confusion failures in JITted code that would lead to a potentially exp crash. This vulnerability affects Firefox < 91 and Thunderbird < 91.
CVE-2021-37711	Versions prior to 6.4.3.1 contain an authenticated server-side request forgery vulnerability in file upload via URL. Version 6.4.3.1 contains a patch. As workarounds for versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin.
CVE-2021-37343	A path traversal vulnerability exists in Nagios XI below version 5.8.5 AutoDiscovery component and could lead to post authenticated RCE under security context of the running Nagios.
CVE-2020-13588	An exploitable SQL injection vulnerability exists in the ‘entities/fields’ page of the Rukovoditel Project Management App 2.7.2. The heading_field_id parameter in ‘‘entitie page is vulnerable to authenticated SQL injection. An attacker can make authenticated HTTP requests to trigger this vulnerability, this can be done either with administr credentials or through cross-site request forgery.
CVE-2020-13589	An exploitable SQL injection vulnerability exists in the ‘entities/fields’ page of the Rukovoditel Project Management App 2.7.2. The entities_id parameter in the 'entities/f (mulitple_edit or copy_selected or export function) is vulnerable to authenticated SQL injection. An attacker can make authenticated HTTP requests to trigger this vulne this can be done either with administrator credentials or through cross-site request forgery.
CVE-2020-24576	Netskope Client through 77 allows low-privileged users to elevate their privileges to NT AUTHORITY\SYSTEM.
CVE-2021-37694	@asyncapi/java-spring-cloud-stream-template generates a Spring Cloud Stream (SCSt) microservice. In versions prior to 0.7.0 arbitrary code injection was possible wh attacker controls the AsyncAPI document. An example is provided in GHSA-xj6r-2jpm-qvxp. There are no mitigations available and all users are advised to update.
CVE-2021-38518	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects RAX200 before 1.0.4.120, RAX75 before 1.0.4.120, RAX80 before RBK852 before 3.2.17.12, RBR850 before 3.2.17.12, and RBS850 before 3.2.17.12.
CVE-2021-37639	TensorFlow is an end-to-end open source platform for machine learning. When restoring tensors via raw APIs, if the tensor name is not provided, TensorFlow can be tr dereferencing a null pointer. Alternatively, attackers can read memory outside the bounds of heap allocated data by providing some tensor names but not enough for a restoration. The [implementation] (https://github.com/tensorflow/tensorflow/blob/47a06f40411a69c99f381495f490536972152ac0/tensorflow/core/kernels/save_restore_tensor.cc#L158-L159) retrieves th list corresponding to the `tensor_name` user controlled input and immediately retrieves the tensor at the restoration index (controlled via `preferred_shard` argument). T without validating that the provided list has enough values. If the list is empty this results in dereferencing a null pointer (undefined behavior). If, however, the list has so elements, if the restoration index is outside the bounds this results in heap OOB read. We have patched the issue in GitHub commit 9e82dce6e6bd1f36a57e08fa85af213e2b2f2622. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4. TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-28372	ThroughTek's Kalay Platform 2.0 network allows an attacker to impersonate an arbitrary ThroughTek (TUTK) device given a valid 20-byte uniquely assigned identifier (could result in an attacker hijacking a victim's connection and forcing them into supplying credentials needed to access the victim TUTK device.
CVE-2021-38529	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900 befor and R9000 before 1.0.4.26.
CVE-2021-21594	Dell PowerScale OneFS versions 8.2.2 - 9.1.0.x contain a use of get request method with sensitive query strings vulnerability. It can lead to potential disclosure of sens Dell recommends upgrading at your earliest opportunity.
CVE-2021-38588	In cPanel before 96.0.13, fix_cpanel_perl lacks verification of the integrity of downloads (SEC-587).

CVE Number	Description
CVE-2021-29986	A suspected race condition when calling getaddrinfo led to memory corruption and a potentially exploitable crash. *Note: This issue only affected Linux operating syster operating systems are unaffected.* This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
CVE-2021-34524	Microsoft Dynamics 365 On-Premises Remote Code Execution Vulnerability
CVE-2021-36982	AIMANAGER before B115 on MONITORAPP Application Insight Web Application Firewall (AIWAF) devices with Manager 2.1.0 allows OS Command Injection because input validation on one of the parameters of an HTTP request.
CVE-2021-38589	In cPanel before 96.0.13, scripts/fix-cpanel-perl does not properly restrict the overwriting of files (SEC-588).
CVE-2020-29548	An issue was discovered in SmarterTools SmarterMail through 100.0.7537. Meddler-in-the-middle attackers can pipeline commands after a POP3 STLS command, inje plaintext commands into an encrypted user session.
CVE-2021-36278	Dell EMC PowerScale OneFS versions 8.2.x, 9.1.0.x, and 9.1.1.1 contain a sensitive information exposure vulnerability in log files. A local malicious user with ISI_PRIV_LOGIN_SSH, ISI_PRIV_LOGIN_CONSOLE, or ISI_PRIV_SYS_SUPPORT privileges may exploit this vulnerability to access sensitive information. If any thir consumes those logs, the same sensitive information is available to those systems as well.
CVE-2021-38527	Certain NETGEAR devices are affected by command injection by an unauthenticated attacker. This affects CBR40 before 2.5.0.14, EX6100v2 before 1.0.1.98, EX6150 1.0.1.98, EX6250 before 1.0.0.132, EX6400 before 1.0.2.158, EX6400v2 before 1.0.0.132, EX6410 before 1.0.0.132, EX6420 before 1.0.0.132, EX7300 before 1.0.2.1 EX7300v2 before 1.0.0.132, EX7320 before 1.0.0.132, EX7700 before 1.0.0.216, EX8000 before 1.0.1.232, R7800 before 1.0.2.78, RBK12 before 2.6.1.44, RBR10 bef 2.6.1.44, RBS10 before 2.6.1.44, RBK20 before 2.6.1.38, RBR20 before 2.6.1.36, RBS20 before 2.6.1.38, RBK40 before 2.6.1.38, RBR40 before 2.6.1.36, RBS40 befc 2.6.1.38, RBK50 before 2.6.1.40, RBR50 before 2.6.1.40, RBS50 before 2.6.1.40, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, RBS750 before 3.2.16.6, RBK852 3.2.16.6, RBR850 before 3.2.16.6, RBS850 before 3.2.16.6, RBS40V before 2.6.2.4, RBS50Y before 2.6.1.40, RBW30 before 2.6.2.2, and XR500 before 2.3.2.114.
CVE-2021-37710	Shopware is an open source eCommerce platform. Versions prior to 6.4.3.1 contain a Cross-Site Scripting vulnerability via SVG media files. Version 6.4.3.1 contains a workarounds for older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin.
CVE-2021-37627	Contao is an open source CMS that allows creation of websites and scalable web applications. In affected versions it is possible to gain privileged rights in the Contao I Installations are only affected if they have untrusted back end users who have access to the form generator. All users are advised to update to Contao 4.4.56, 4.9.18 or a workaround users may disable the form generator or disable the login for untrusted back end users.
CVE-2020-18458	Cross Site Request Forgery (CSRF) vulnerability exists in DamiCMS v6.0.6 that can add an admin account via admin.php?s=/Admin/doadd.
CVE-2020-28594	A use-after-free vulnerability exists in the _3MF_Importer::_handle_end_model() functionality of Prusa Research PrusaSlicer 2.2.0 and Master (commit 4b040b856). A crafted 3MF file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.
CVE-2021-34533	Windows Graphics Component Font Parsing Remote Code Execution Vulnerability
CVE-2021-34530	Windows Graphics Component Remote Code Execution Vulnerability
CVE-2021-37347	Nagios XI before version 5.8.5 is vulnerable to local privilege escalation because getprofile.sh does not validate the directory name it receives as an argument.
CVE-2021-37349	Nagios XI before version 5.8.5 is vulnerable to local privilege escalation because cleaner.php does not sanitise input read from the database.
CVE-2021-34486	Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-34484	Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2021-34483	Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-34478	Microsoft Office Remote Code Execution Vulnerability

CVE Number	Description
CVE-2021-26431	Windows Recovery Environment Agent Elevation of Privilege Vulnerability
CVE-2021-0640	In noteAtomLogged of StatsdStats.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no ac execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-9Android ID: A-187957589
CVE-2021-26425	Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-0646	In sqlite3_str_vappendf of sqlite3.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege if the user ca inject a printf into a privileged process's SQL with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: A Android-10 Android-11 Android-8.1Android ID: A-153352319
CVE-2021-0645	In shouldBlockFromTree of ExternalStorageProvider.java, there is a possible permissions bypass. This could lead to local escalation of privilege, allowing an app to rea app directories in external storage, which should be restricted in Android 11, with no additional execution privileges needed. User interaction is needed for exploitation.F AndroidVersions: Android-11Android ID: A-157320644
CVE-2021-34398	NVIDIA DCGM, all versions prior to 2.2.9, contains a vulnerability in the DIAG module where any user can inject shared libraries into the DCGM server, which is usuall as root, which may lead to privilege escalation, total loss of confidentiality and integrity, and complete denial of service.
CVE-2021-34536	Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-25263	Local privilege vulnerability in Yandex Browser for Windows prior to 21.9.0.390 allows a local, low privileged, attacker to execute arbitary code with the SYSTEM privile through manipulating files in directory with insecure permissions during Yandex Browser update process.
CVE-2021-27794	A vulnerability in the authentication mechanism of Brocade Fabric OS versions before Brocade Fabric OS v.9.0.1a, v8.2.3a and v7.4.2h could allow a user to Login with password, and invalid password through telnet, ssh and REST.
CVE-2021-27792	The request handling functions in web management interface of Brocade Fabric OS versions before v9.0.1a, v8.2.3a, and v7.4.2h do not properly handle malformed us resulting in a service crash. An authenticated attacker could use this weakness to cause the FOS HTTP application handler to crash, requiring a reboot.
CVE-2021-21812	A stack-based buffer overflow vulnerability exists in the command-line-parsing HandleFileArg functionality of AT&T Labs' Xmill 0.7. Within the function HandleFileArg th argument filepattern is under control of the user who passes it in from the command line. filepattern is passed directly to strcpy copying the path provided by the user in sized buffer without any length checks resulting in a stack-buffer overflow. An attacker can provide malicious input to trigger these vulnerabilities.
CVE-2021-27790	The command ipfilter in Brocade Fabric OS before Brocade Fabric OS v.9.0.1a, v8.2.3, and v8.2.0_CBN4, and v7.4.2h uses unsafe string function to process user inpu Authenticated attackers can abuse this vulnerability to exploit stack-based buffer overflows, allowing execution of arbitrary code as the root user account.
CVE-2021-36280	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.x contain an incorrect permission assignment for critical resource vulnerability. This could allow a user with ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE to access privileged information about the cluster.
CVE-2021-38088	Acronis Cyber Protect 15 for Windows prior to build 27009 allowed local privilege escalation via binary hijacking.
CVE-2021-38086	Acronis Cyber Protect 15 for Windows prior to build 27009 and Acronis Agent for Windows prior to build 26226 allowed local privilege escalation via DLL hijacking.
CVE-2021-37841	Docker Desktop before 3.6.0 suffers from incorrect access control. If a low-privileged account is able to access the server running the Windows containers, it can lead t container compromise in both process isolation and Hyper-V isolation modes. This security issue leads an attacker with low privilege to read, write and possibly even e code inside the containers.
CVE-2021-37666	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null p `tf.raw_ops.RaggedTensorToVariant`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/ragged_tensor_to_variant_op.cc#L129) has an i validation of the splits values, missing the case when the argument would be empty. We have patched the issue in GitHub commit be7a4de6adfbd303ce08be4332554dff70362612. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4 TensorFlow 2.3.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-34537	Windows Bluetooth Driver Elevation of Privilege Vulnerability
CVE-2021-37652	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation for `tf.raw_ops.BoostedTreesCreateEnsemble` can re use after free error if an attacker supplies specially crafted arguments. The [implementation] (https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/boosted_trees/resource_ops.cc#L55) uses a ref counted resource and decrements the refcount if the initialization fails, as it should. However, when the code was written, the resource was represented as a naked poi later refactoring has changed it to be a smart pointer. Thus, when the pointer leaves the scope, a subsequent `free`-ing of the resource occurs, but this fails to take into that the refcount has already reached 0, thus the resource has been already freed. During this double-free process, members of the resource object are accessed for c they are invalid as the entire resource has been freed. We have patched the issue in GitHub commit 5ecec9c6fbdbc6be03295685190a45e7eee726ab. The fix will be in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported r
CVE-2021-3708	D-Link router DSL-2750U with firmware vME1.16 or prior versions is vulnerable to OS command injection. An unauthenticated attacker on the local network may exploi CVE-2021-3707, to execute any OS commands on the vulnerable device.
CVE-2021-37648	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the code for `tf.raw_ops.SaveV2` does not properly validate the inputs an attacker can trigger a null pointer dereference. The [implementation] (https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/save_restore_v2_ops.cc) uses `ValidateInputs` t that the input arguments are valid. This validation would have caught the illegal state represented by the reproducer above. However, the validation uses `OP_REQUIR translates to setting the `Status` object of the current `OpKernelContext` to an error status, followed by an empty `return` statement which just terminates the execution function it is present in. However, this does not mean that the kernel execution is finalized: instead, execution continues from the next line in `Compute` that follows the `ValidateInputs`. This is equivalent to lacking the validation. We have patched the issue in GitHub commit 9728c60e136912a12d99ca56e106b7cce7af5986. The fix will included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in range.
CVE-2021-37667	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null p `tf.raw_ops.UnicodeEncode`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/unicode_ops.cc#L533-L539) reads the first dime the `input_splits` tensor before validating that this tensor is not empty. We have patched the issue in GitHub commit 2e0ee46f1a47675152d3d865797a18358881d7a6. be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still supported range.
CVE-2021-0576	In flv extractor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privile needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187236084
CVE-2021-37671	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null p `tf.raw_ops.Map*` and `tf.raw_ops.OrderedMap*` operations. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/map_stage_op.cc#L222-L248) has a check in pl ensure that `indices` is in ascending order, but does not check that `indices` is not empty. We have patched the issue in GitHub commit 532f5c5a547126c634fefd43bbad1dc6417678ac. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4 TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-38608	Incorrect Access Control in Tranquil WAPT Enterprise - before 1.8.2.7373 and before 2.0.0.9450 allows guest OS users to escalate privileges via WAPT Agent.
CVE-2021-37650	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation for `tf.raw_ops.ExperimentalDatasetToTFRecord` and `tf.raw_ops.DatasetToTFRecord` can trigger heap buffer overflow and segmentation fault. The [implementation] (https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/data/experimental/to_tf_record_op.cc#L93-L102 that all records in the dataset are of string type. However, there is no check for that, and the example given above uses numeric types. We have patched the issue in G commit e0b6e58c328059829c3eb968136f17aa72b6c876. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, Tenso 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37676	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null p `tf.raw_ops.SparseFillEmptyRows`. The shape inference [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/ops/sparse_ops.cc#L608-L634) does not validate that th arguments are not empty tensors. We have patched the issue in GitHub commit 578e634b4f1c1c684d4b4294f9e5281b2133b3ed. The fix will be included in TensorFlo will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37681	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of SVDF in TFLite is [vulnerable to a null pointer error] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/svdf.cc#L300-L313). The [`GetVariableInput` func (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/kernel_util.cc#L115-L119) can return a null pointe `GetTensorData` assumes that the argument is always a valid tensor. Furthermore, because `GetVariableInput` calls [`GetMutableInput`] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/kernel_util.cc#L82-L90) which might return `nullpt `tensor->is_variable` expression can also trigger a null pointer exception. We have patched the issue in GitHub commit 5b048e87e4e55990dae6b547add4dae59f4e1c will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and supported range.

CVE Number	Description
CVE-2021-37689	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can craft a TFLite model that would trigger a null pointer deref which would result in a crash and denial of service. This is caused by the MLIR optimization of `L2NormalizeReduceAxis` operator. The [implementation] (https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/compiler/mlir/lite/transforms/optimize.cc#L67-L70) unconditio dereferences a pointer to an iterator to a vector without checking that the vector has elements. We have patched the issue in GitHub commit d6b57f461b39fd1aa8c1b870f1b974aac3554955. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4 TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37663	TensorFlow is an end-to-end open source platform for machine learning. In affected versions due to incomplete validation in `tf.raw_ops.QuantizeV2`, an attacker can t undefined behavior via binding a reference to a null pointer or can access data outside the bounds of heap allocated arrays. The [implementation] (https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/quantize_op.cc#L59) has some validation but d check that `min_range` and `max_range` both have the same non-zero number of elements. If `axis` is provided (i.e., not `-1`), then validation should check that it is a v range for the rank of `input` tensor and then the lengths of `min_range` and `max_range` inputs match the `axis` dimension of the `input` tensor. We have patched the i GitHub commit 6da6620efad397c85493b8f8667b821403516708. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37665	TensorFlow is an end-to-end open source platform for machine learning. In affected versions due to incomplete validation in MKL implementation of requantization, an can trigger undefined behavior via binding a reference to a null pointer or can access data outside the bounds of heap allocated arrays. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/mkl/mkl_requantization_range_per_channel_op. not validate the dimensions of the `input` tensor. A similar issue occurs in `MklRequantizePerChannelOp`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/mkl/mkl_requantize_per_channel_op.cc) does n full validation for all the input arguments. We have patched the issue in GitHub commit 9e62869465573cb2d9b5053f1fa02a81fce21d69 and in the Github commit 203214568f5bc237603dbab6e1fd389f1572f5c9. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4. TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-23422	This affects the package bikeshed before 3.0.0. This can occur when an untrusted source file containing Inline Tag Command metadata is processed. When an arbitrar command is executed, the command output would be included in the HTML output.
CVE-2021-36958	A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully e this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with fu rights.
CVE-2021-37345	Nagios XI before version 5.8.5 is vulnerable to local privilege escalation because xi-sys.cfg is being imported from the var directory for some scripts with elevated perm
CVE-2021-0574	In asf extractor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privile needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187234876
CVE-2021-36948	Windows Update Medic Service Elevation of Privilege Vulnerability
CVE-2021-36279	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.x contain an incorrect permission assignment for critical resource vulnerability. This could allow a user with ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE to access privileged information about the cluster.
CVE-2021-21815	A stack-based buffer overflow vulnerability exists in the command-line-parsing HandleFileArg functionality of AT&T Labs' Xmill 0.7. Within the function HandleFileArg th argument filepattern is under control of the user who passes it in from the command line. filepattern is passed directly to strcpy copying the path provided by the user in sized buffer without any length checks resulting in a stack-buffer overflow. An attacker can provide malicious input to trigger this vulnerability.
CVE-2021-21814	Within the function HandleFileArg the argument filepattern is under control of the user who passes it in from the command line. filepattern is passed directly to strlen to the ending location of the char* passed in by the user, no checks are done to see if the passed in char* is longer than the staticly sized buffer data is memcpy'd into, bu memcpy a null byte is written to what is assumed to be the end of the buffer to terminate the char*, but without length checks, this null write occurs at an arbitrary offset buffer. An attacker can provide malicious input to trigger this vulnerability.
CVE-2021-0593	In sendDevicePickedIntent of DevicePickerFragment.java, there is a possible way to invoke a privileged broadcast receiver due to a confused deputy. This could lead t escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android- Android-9Android ID: A-179386068
CVE-2021-36941	Microsoft Word Remote Code Execution Vulnerability
CVE-2021-36937	Windows Media MPEG-4 Video Decoder Remote Code Execution Vulnerability
CVE-2021-21813	Within the function HandleFileArg the argument filepattern is under control of the user who passes it in from the command line. filepattern is passed directly to memcpy the path provided by the user into a staticly sized buffer without any length checks resulting in a stack-buffer overflow.
CVE-2021-36927	Windows Digital TV Tuner device registration application Elevation of Privilege Vulnerability

CVE Number	Description
CVE-2021-0573	In asf extractor, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privile needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187231635
CVE-2021-0519	In BITSTREAM_FLUSH of ih264e_bitstream.h, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local information disclosure with additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android I 176533109
CVE-2021-37688	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can craft a TFLite model that would trigger a null pointer deref which would result in a crash and denial of service. The [implementation] (https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/internal/optimized/optimized_ops.h#L268-L285) unconditionally dereferences a pointer. We have patched the issue in GitHub commit 15691e456c7dc9bd6be203b09765b063bf4a380c. The fix will be included in Tens 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-34471	Microsoft Windows Defender Elevation of Privilege Vulnerability
CVE-2021-32947	FATEK Automation FvDesigner, Versions 1.5.88 and prior is vulnerable to a stack-based buffer overflow, which may allow an attacker to execute arbitrary code.
CVE-2021-0196	Improper access control in kernel mode driver for some Intel(R) NUC 9 Extreme Laptop Kits before version 2.2.0.20 may allow an authenticated user to potentially enat escalation of privilege via local access.
CVE-2020-25561	SapphireIMS 5 utilized default sapphire:ims credentials to connect the client to server. This credential is saved in ServerConf.config file in the client.
CVE-2021-32439	Buffer overflow in the stbl_AppendSize function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file.
CVE-2021-32939	FATEK Automation FvDesigner, Versions 1.5.88 and prior is vulnerable to an out-of-bounds write while processing project files, allowing an attacker to craft a project fil permit arbitrary code execution.
CVE-2021-38571	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows DLL hijacking, aka CNVD-C-2021-68000 and CNVD-C-2021-68502.
CVE-2021-32931	An uninitialized pointer in FATEK Automation FvDesigner, Versions 1.5.88 and prior may be exploited while the application is processing project files, allowing an attacl a special project file that may permit arbitrary code execution.
CVE-2021-36770	Encode.pm, as distributed in Perl through 5.34.0, allows local users to gain privileges via a Trojan horse Encode::ConfigLocal library (in the current working directory) th preempts dynamic module loading. Exploitation requires an unusual configuration, and certain 2021 versions of Encode.pm (3.05 through 3.11). This issue occurs beca operator evaluates @INC in a scalar context, and thus @INC has only an integer value.
CVE-2021-38085	The Canon TR150 print driver through 3.71.2.10 is vulnerable to a privilege escalation issue. During the add printer process, a local attacker can overwrite CNMurGE.d timed properly, the overwritten DLL will be loaded into a SYSTEM process resulting in escalation of privileges. This occurs because the driver drops a world-writable DL CanonBJ %PROGRAMDATA% location that gets loaded by printisolationhost (a system process).
CVE-2021-0160	Uncontrolled search path in some Intel(R) NUC Pro Chassis Element AverMedia Capture Card drivers before version 3.0.64.143 may allow an authenticated user to po enable escalation of privilege via local access.
CVE-2021-0084	Improper input validation in the Intel(R) Ethernet Controllers X722 and 800 series Linux RMDA driver before version 1.3.19 may allow an authenticated user to potentia escalation of privilege via local access.
CVE-2021-0062	Improper input validation in some Intel(R) Graphics Drivers before version 27.20.100.8935 may allow an authenticated user to potentially enable escalation of privilege access.
CVE-2021-0061	Improper initialization in some Intel(R) Graphics Driver before version 27.20.100.9030 may allow an authenticated user to potentially enable escalation of privilege via l access.
CVE-2021-1107	NVIDIA Linux kernel distributions contain a vulnerability in nvmap NVMAP_IOC_WRITE* paths, where improper access controls may lead to code execution, complete service, and seriously compromised integrity of all system components.
CVE-2021-1106	NVIDIA Linux kernel distributions contain a vulnerability in nvmap, where writes may be allowed to read-only buffers, which may result in escalation of privileges, compl of service, unconstrained information disclosure, and serious data tampering of all processes on the system.

CVE Number	Description
CVE-2021-26429	Azure Sphere Elevation of Privilege Vulnerability
CVE-2021-37637	TensorFlow is an end-to-end open source platform for machine learning. It is possible to trigger a null pointer dereference in TensorFlow by passing an invalid input to `tf.raw_ops.CompressElement`. The [implementation](https://github.com/tensorflow/tensorflow/blob/47a06f40411a69c99f381495f490536972152ac0/tensorflow/core/data/compression_utils.cc#L34) was accessing the size obtained from the return of a separate function call before validating that said buffer is valid. We have patched the issue in GitHub commit 5dc7f6981fdaf74c8c5be41f393df705841fb7c5. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3 TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37638	TensorFlow is an end-to-end open source platform for machine learning. Sending invalid argument for `row_partition_types` of `tf.raw_ops.RaggedTensorToTensor` AP a null pointer dereference and undefined behavior. The [implementation](https://github.com/tensorflow/tensorflow/blob/47a06f40411a69c99f381495f490536972152ac0/tensorflow/core/kernels/ragged_tensor_to_tensor_op.cc#L328) accesses element of a user supplied list of values without validating that the provided list is not empty. We have patched the issue in GitHub commit 301ae88b331d37a2a16159b65b255f4f9eb39314. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4 TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37643	TensorFlow is an end-to-end open source platform for machine learning. If a user does not provide a valid padding value to `tf.raw_ops.MatrixDiagPartOp`, then the co a null pointer dereference (if input is empty) or produces invalid behavior, ignoring all values after the first. The [implementation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/linalg/matrix_diag_op.cc#L89) reads the first valu tensor buffer without first checking that the tensor has values to read from. We have patched the issue in GitHub commit 482da92095c4d48f8784b1f00dda4f81c28d29 will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and supported range.
CVE-2021-37647	TensorFlow is an end-to-end open source platform for machine learning. When a user does not supply arguments that determine a valid sparse tensor, `tf.raw_ops.SparseTensorSliceDataset` implementation can be made to dereference a null pointer. The [implementation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/data/sparse_tensor_slice_dataset_op.cc#L240-L some argument validation but fails to consider the case when either `indices` or `values` are provided for an empty sparse tensor when the other is not. If `indices` is er [code that performs validation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/data/sparse_tensor_slice_dataset_op.cc#L260-L checking that the indices are monotonically increasing) results in a null pointer dereference. If `indices` as provided by the user is empty, then `indices` in the C++ code backed by an empty `std::vector`, hence calling `indices->dim_size(0)` results in null pointer dereferencing (same as calling `std::vector::at()` on an empty vector). We h patched the issue in GitHub commit 02cc160e29d20631de3859c6653184e3f876b9d7. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37649	TensorFlow is an end-to-end open source platform for machine learning. The code for `tf.raw_ops.UncompressElement` can be made to trigger a null pointer dereferen [implementation](https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/data/experimental/compression_ops.cc#L50-L5 pointer to a `CompressedElement` from a `Variant` tensor and then proceeds to dereference it for decompressing. There is no check that the `Variant` tensor containec `CompressedElement`, so the pointer is actually `nullptr`. We have patched the issue in GitHub commit 7bdf50bb4f5c54a4997c379092888546c97c3ebd. The fix will be in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supporte
CVE-2021-23420	This affects the package codeception/codeception from 4.0.0 and before 4.1.22, before 3.1.3. The RunProcess class can be leveraged as a gadget to run arbitrary com a system that is deserializing user input without validation.
CVE-2021-32808	ckeditor is an open source WYSIWYG HTML editor with rich content support. A vulnerability has been discovered in the clipboard Widget plugin if used alongside the u feature. The vulnerability allows a user to abuse undo functionality using malformed widget HTML, which could result in executing JavaScript code. It affects all users u CKEditor 4 plugins listed above at version >= 4.13.0. The problem has been recognized and patched. The fix will be available in version 4.16.2.
CVE-2021-36940	Microsoft SharePoint Server Spoofing Vulnerability
CVE-2017-16629	In SapphireIMS 4097_1, it is possible to guess the registered/active usernames of the software from the errors it gives out for each type of user on the Login form. For ' User" - it gives an error "The application failed to identify the user. Please contact administrator for help." For "Correct User and Incorrect Password" - it gives an error "Authentication failed. Please login again."
CVE-2021-38712	OneNav 0.9.12 allows Information Disclosure of the onenav.db3 contents. NOTE: the vendor's recommended solution is to block the access via an NGINX configuratio
CVE-2021-36933	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2021-36932	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2021-38758	Directory traversal vulnerability in Online Catering Reservation System 1.0 exists due to lack of validation in index.php.

CVE Number	Description
CVE-2021-36942	Windows LSA Spoofing Vulnerability
CVE-2021-22932	An issue has been identified in the CTX269106 mitigation tool for Citrix ShareFile storage zones controller which causes the ShareFile file encryption option to become it had previously been enabled. Customers are only affected by this issue if they previously selected “Enable Encryption” in the ShareFile configuration page and did nc this setting after running the CTX269106 mitigation tool. ShareFile customers who have not run the CTX269106 mitigation tool or who re-selected “Enable Encryption” immediately after running the tool are unaffected by this issue.
CVE-2021-36926	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2021-38587	In cPanel before 96.0.13, scripts/fix-cpanel-perl mishandles the creation of temporary files (SEC-586).
CVE-2021-39131	ced detects character encoding using Google’s compact_enc_det library. In ced v0.1.0, passing data types other than `Buffer` causes the Node.js process to crash. Th has been patched in ced v1.0.0. As a workaround, before passing an argument to ced, verify it’s a `Buffer` using `Buffer.isBuffer(obj)`.
CVE-2021-36793	The routes (aka Extbase Yaml Routes) extension before 2.1.1 for TYPO3, when CsrfTokenViewHelper is used, allows Sensitive Information Disclosure because a sess identifier is unsafely present in HTML output.
CVE-2021-38623	The deferred_image_processing (aka Deferred image processing) extension before 1.0.2 for TYPO3 allows Denial of Service via the FAL API because of /var/transient consumption.
CVE-2021-37348	Nagios XI before version 5.8.5 is vulnerable to local file inclusion through improper limitation of a pathname in index.php.
CVE-2021-33056	Belledonne Belle-sip before 4.5.20, as used in Linphone and other products, can crash via an invalid From header in a SIP message.
CVE-2021-0284	A buffer overflow vulnerability in the TCP/IP stack of Juniper Networks Junos OS allows an attacker to send specific sequences of packets to the device thereby causin of Service (DoS). By repeatedly sending these sequences of packets to the device, an attacker can sustain the Denial of Service (DoS) condition. The device will abnor down as a result of these sent packets. A potential indicator of compromise will be the following message in the log files: "eventd[13955]: SYSTEM_ABNORMAL_SHU System abnormally shut down" This issue is only triggered by traffic destined to the device. Transit traffic will not trigger this issue. This issue affects: Juniper Networks 12.3 versions prior to 12.3R12-S19; 15.1 versions prior to 15.1R7-S10; 17.3 versions prior to 17.3R3-S12; 18.4 versions prior to 18.4R2-S9, 18.4R3-S9; 19.1 versions p 19.1R3-S7; 19.2 versions prior to 19.2R1-S7, 19.2R3-S3; 19.3 versions prior to 19.3R2-S7, 19.3R3-S3; 19.4 versions prior to 19.4R3-S5; 20.1 versions prior to 20.1R3 versions prior to 20.2R3-S2; 20.3 versions prior to 20.3R3-S1; 20.4 versions prior to 20.4R2-S2, 20.4R3; 21.1 versions prior to 21.1R2; 21.2 versions prior to 21.2R1-S
CVE-2021-20427	IBM Security Guardium 11.2 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 196314.
CVE-2021-38614	Polipo through 1.1.1, when NDEBUG is used, allows a heap-based buffer overflow during parsing of a Range header. NOTE: This vulnerability only affects products tha longer supported by the maintainer
CVE-2021-22940	Node.js before 16.6.1, 14.17.5, and 12.22.5 is vulnerable to a use after free attack where an attacker might be able to exploit the memory corruption, to change process
CVE-2020-23334	A WRITE memory access in the AP4_NullTerminatedStringAtom::AP4_NullTerminatedStringAtom component of Bento4 version 06c39d9 can lead to a segmentation fa
CVE-2020-23333	A heap-based buffer overflow exists in the AP4_CttsAtom::AP4_CttsAtom component located in /Core/Ap4Utils.h of Bento4 version 06c39d9. This can lead to a denial (DOS).
CVE-2020-23332	A heap-based buffer overflow exists in the AP4_StdcFileByteStream::ReadPartial component located in /StdC/Ap4StdCFileByteStream.cpp of Bento4 version 06c39d9 can lead to a denial of service (DOS).
CVE-2020-23331	An issue was discovered in Bento4 version 06c39d9. A NULL pointer dereference exists in the AP4_DescriptorListWriter::Action component located in /Core/Ap4Descr allows an attacker to cause a denial of service (DOS).
CVE-2020-23330	An issue was discovered in Bento4 version 06c39d9. A NULL pointer dereference exists in the AP4_Stz2Atom::GetSampleSize component located in /Core/Ap4Stz2At allows an attacker to cause a denial of service (DOS).

CVE Number	Description
CVE-2021-38711	In gitit before 0.15.0.0, the Export feature can be exploited to leak information from files.
CVE-2017-16632	In SapphireIMS 4097_1, the password in the database is stored in Base64 format.
CVE-2021-33193	A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects HTTP Server 2.4.17 to 2.4.48.
CVE-2020-18757	An issue in Dut Computer Control Engineering Co.'s PLC MAC1100 allows attackers to cause persistent denial of service (DOS) via a crafted packet.
CVE-2021-26433	Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2020-18754	An information disclosure vulnerability exists within Dut Computer Control Engineering Co.'s PLC MAC1100.
CVE-2020-18756	An arbitrary memory access vulnerability in the EPA protocol of Dut Computer Control Engineering Co.'s PLC MAC1100 allows attackers to read the contents of any va area.
CVE-2021-38565	An issue was discovered in Foxit PDF Reader before 11.0.1 and PDF Editor before 11.0.1. It allows writing to arbitrary files via submitForm.
CVE-2021-35392	Realtek Jungle SDK version v2.x up to v3.4.14B provides a 'WiFi Simple Config' server that implements both UPnP and SSDP protocols. The binary is usually named v mini_upnpd and is the successor to miniigd. The server is vulnerable to a heap buffer overflow that is present due to unsafe crafting of SSDP NOTIFY messages from r SEARCH messages ST header.
CVE-2020-18759	An information disclosure vulnerability exists in the EPA protocol of Dut Computer Control Engineering Co.'s PLC MAC1100.
CVE-2021-26423	.NET Core and Visual Studio Denial of Service Vulnerability
CVE-2021-38604	In librt in the GNU C Library (aka glibc) through 2.34, sysdeps/unix/sysv/linux/mq_notify.c mishandles certain NOTIFY_REMOVED data, leading to a NULL pointer dere NOTE: this vulnerability was introduced as a side effect of the CVE-2021-33574 fix.
CVE-2021-38593	Qt 5.x before 5.15.6 and 6.x through 6.1.2 has an out-of-bounds write in QOutlineMapper::convertPath (called from QRasterPaintEngine::fill and QPaintEngineEx::strok
CVE-2021-38599	WAL-G before 1.1, when a non-libsodium build (e.g., one of the official binary releases published as GitHub Releases) is used, silently ignores the libsodium encryption uploads cleartext backups. This is arguably a Principle of Least Surprise violation because "the user likely wanted to encrypt all file activity."
CVE-2021-38592	Wasm3 0.5.0 has a heap-based buffer overflow in op_Const64 (called from EvaluateExpression and m3_LoadModule).
CVE-2021-36786	The miniorange_saml (aka Miniorange Saml) extension before 1.4.3 for TYPO3 allows Sensitive Data Exposure of API credentials and private keys.
CVE-2021-38291	FFmpeg version (git commit de8e6e67e7523e48bb27ac224a0b446df05e1640) suffers from a an assertion failure at src/libavutil/mathematics.c.
CVE-2020-20981	A SQL injection in the /admin/?n=logs&c=index&a=dolist component of Metinfo 7.0 allows attackers to access sensitive database information.
CVE-2021-38569	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.4. It allows stack consumption via recursive function calls during the handling of XFA forms or l

CVE Number	Description
CVE-2021-38567	An issue was discovered in Foxit PDF Editor before 11.0.1 and PDF Reader before 11.0.1 on macOS. It mishandles missing dictionary entries, leading to a NULL point dereference, aka CNVD-C-2021-95204.
CVE-2021-39242	An issue was discovered in HAProxy 2.2 before 2.2.16, 2.3 before 2.3.13, and 2.4 before 2.4.3. It can lead to a situation with an attacker-controlled HTTP Host header, mismatch between Host and authority is mishandled.
CVE-2021-38566	An issue was discovered in Foxit PDF Reader before 11.0.1 and PDF Editor before 11.0.1. It allows stack consumption during recursive processing of embedded XML
CVE-2021-39240	An issue was discovered in HAProxy 2.2 before 2.2.16, 2.3 before 2.3.13, and 2.4 before 2.4.3. It does not ensure that the scheme and path portions of a URI have the characters. For example, the authority field (as observed on a target HTTP/2 server) might differ from what the routing rules were intended to achieve.
CVE-2021-36281	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.x contain an incorrect permission assignment vulnerability. A low privileged authenticated user can potentially exploit vulnerability to escalate privileges.
CVE-2021-38515	Certain NETGEAR devices are affected by denial of service. This affects R6400v2 before 1.0.4.98, R6700v3 before 1.0.4.98, R7900 before 1.0.3.18, and R8000 before
CVE-2021-0591	In sendReplyIntentToReceiver of BluetoothPermissionActivity.java, there is a possible way to invoke privileged broadcast receivers due to a confused deputy. This coul local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android- Android-8.1Android ID: A-179386960
CVE-2021-36945	Windows 10 Update Assistant Elevation of Privilege Vulnerability
CVE-2021-37641	TensorFlow is an end-to-end open source platform for machine learning. In affected versions if the arguments to `tf.raw_ops.RaggedGather` don't determine a valid rag code can trigger a read from outside of bounds of heap allocated buffers. The [implementation] (https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/ragged_gather_op.cc#L70) directly reads the firs dimension of a tensor shape before checking that said tensor has rank of at least 1 (i.e., it is not a scalar). Furthermore, the implementation does not check that the list `params_nested_splits` is not an empty list of tensors. We have patched the issue in GitHub commit a2b743f6017d7b97af1fe49087ae15f0ac634373. The fix will be inc TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported r
CVE-2021-37695	ckeditor is an open source WYSIWYG HTML editor with rich content support. A potential vulnerability has been discovered in CKEditor 4 [Fake Objects] (https://ckeditor.com/cke4/addon/fakeobjects) package. The vulnerability allowed to inject malformed Fake Objects HTML, which could result in executing JavaScript co affects all users using the CKEditor 4 plugins listed above at version < 4.16.2. The problem has been recognized and patched. The fix will be available in version 4.16.2
CVE-2021-37635	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of sparse reduction operations in TensorFlow can trig accesses outside of bounds of heap allocated data. The [implementation] (https://github.com/tensorflow/tensorflow/blob/a1bc56203f21a5a4995311825ffaba7a670d7747/tensorflow/core/kernels/sparse_reduce_op.cc#L217-L228) fails to valida each reduction group does not overflow and that each corresponding index does not point to outside the bounds of the input tensor. We have patched the issue in GitH 87158f43f05f2720a374f3e6d22a7aaa3a33f750. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4. TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-1108	NVIDIA Linux kernel distributions contain a vulnerability in FuSa Capture (VI/ISP), where integer underflow due to lack of input validation may lead to complete denial o partial integrity, and serious confidentiality loss for all processes in the system.
CVE-2021-3633	A DLL preloading vulnerability was reported in Lenovo Driver Management prior to version 2.9.0719.1104 that could allow privilege escalation.
CVE-2021-37654	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can trigger a crash via a `CHECK`-fail in debug builds of Tens using `tf.raw_ops.ResourceGather` or a read from outside the bounds of heap allocated data in the same API in a release build. The [implementation] (https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/resource_variable_ops.cc#L660-L668) does not the `batch_dims` value that the user supplies is less than the rank of the input tensor. Since the implementation uses several for loops over the dimensions of `tensor`, in reading data from outside the bounds of heap allocated buffer backing the tensor. We have patched the issue in GitHub commit bc9c546ce7015c57c2f15c168b3d9201de679a1d. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4 TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37655	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can trigger a read from outside of bounds of heap allocated da sending invalid arguments to `tf.raw_ops.ResourceScatterUpdate`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/resource_variable_ops.cc#L919-L923) has an ir validation of the relationship between the shapes of `indices` and `updates`: instead of checking that the shape of `indices` is a prefix of the shape of `updates` (so that broadcasting can happen), code only checks that the number of elements in these two tensors are in a divisibility relationship. We have patched the issue in GitHub co 01cff3f986259d661103412a20745928c727326f. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4. TensorFlow 2.3.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-37659	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null p binary cwise operations that don't require broadcasting (e.g., gradients of binary cwise operations). The [implementation] (https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/cwise_ops_common.h#L264) assumes that the have exactly the same number of elements but does not check that. Hence, when the eigen functor executes it triggers heap OOB reads and undefined behavior due to nullptr. We have patched the issue in GitHub commit 93f428fd1768df147171ed674fee1fc5ab8309ec. The fix will be included in TensorFlow 2.6.0. We will also cherrypi commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37664	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can read from outside of bounds of heap allocated data by ser specially crafted illegal arguments to `BoostedTreesSparseCalculateBestFeatureSplit`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/boosted_trees/stats_ops.cc) needs to validate t value in `stats_summary_indices` is in range. We have patched the issue in GitHub commit e84c975313e8e8e38bb2ea118196369c45c51378. The fix will be included i TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported r
CVE-2021-22938	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform command injection via an unsanitized web parameter in th administrator web console.
CVE-2020-18462	File Upload vulnerabilty in AikCms v2.0.0 in poster_edit.php because the background file management office does not verify the uploaded file.
CVE-2021-1109	NVIDIA camera firmware contains a multistep, timing-related vulnerability where an unauthorized modification by camera resources may result in loss of data integrity c service across several streams.
CVE-2021-22934	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator or compromised Pulse Connect Secure device in a load-balanced co to perform a buffer overflow via a malicious crafted web request.
CVE-2021-36792	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 has incorrect Access Control for confirming various applications.
CVE-2021-3617	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow command injection by setting a specially crafted network configuration. This vul the same as CNVD-2020-68652.
CVE-2021-38585	The WHM Locale Upload feature in cPanel before 98.0.1 allows unserialization attacks (SEC-585).
CVE-2021-38584	The WHM Locale Upload feature in cPanel before 98.0.1 allows XXE attacks (SEC-585).
CVE-2021-37626	Contao is an open source CMS that allows you to create websites and scalable web applications. In affected versions it is possible to load PHP files by entering insert t Contao back end. Installations are only affected if they have untrusted back end users who have the rights to modify fields that are shown in the front end. Update to Co 4.4.56, 4.9.18 or 4.11.7 to resolve. If you cannot update then disable the login for untrusted back end users.
CVE-2021-22935	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform command injection via an unsanitized web parameter.
CVE-2021-22937	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform a file write via a maliciously crafted archive uploaded in th administrator web interface.
CVE-2021-37657	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null p operations of type `tf.raw_ops.MatrixDiagV*`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/linalg/matrix_diag_op.cc) has incomplete valida the value of `k` is a valid tensor. We have check that this value is either a scalar or a vector, but there is no check for the number of elements. If this is an empty tensor, that accesses the first element of the tensor is wrong. We have patched the issue in GitHub commit f2a673bd34f0d64b8e40a551ac78989d16daad09. The fix will be inc TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported r
CVE-2021-37679	TensorFlow is an end-to-end open source platform for machine learning. In affected versions it is possible to nest a `tf.map_fn` within another `tf.map_fn` call. However input tensor is a `RaggedTensor` and there is no function signature provided, code assumes the output is a fully specified tensor and fills output buffer with uninitialized from the heap. The `t` and `z` outputs should be identical, however this is not the case. The last row of `t` contains data from the heap which can be used to leak other information. The bug lies in the conversion from a `Variant` tensor to a `RaggedTensor`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/ragged_tensor_from_variant_op.cc#L177-L190) check that all inner shapes match and this results in the additional dimensions. The same implementation can result in data loss, if input tensor is tweaked. We have pa issue in GitHub commit 4e2565483d0ffcadc719bd44893fb7f609bb5f12. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-0002	Improper conditions check in some Intel(R) Ethernet Controllers 800 series Linux drivers before version 1.4.11 may allow an authenticated user to potentially enable inf disclosure or denial of service via local access.

CVE Number	Description
CVE-2021-36949	Microsoft Azure Active Directory Connect Authentication Bypass Vulnerability
CVE-2021-37662	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can generate undefined behavior via a reference binding to nu `BoostedTreesCalculateBestGainsPerFeature` and similar attack can occur in `BoostedTreesCalculateBestFeatureSplitV2`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/boosted_trees/stats_ops.cc) does not validate t values. We have patched the issue in GitHub commit 9c87c32c710d0b5b53dc6fd3bfde4046e1f7a5ad and in commit 429f009d2b2c09028647dd4bb7b3f6f414bbaad7. be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still supported range.
CVE-2021-37696	tmerc-cogs are a collection of open source plugins for the Red Discord bot. A vulnerability has been found in the code that allows any user to access sensitive informati crafting a specific MassDM message. Issue is patched in commit 92325be650a6c17940cc52611797533ed95dbbe1. All users are advised to update to the current comm workaround users may unload the MassDM cog or globally disable the `[p]massdm` command.
CVE-2021-1110	NVIDIA Linux kernel distributions on Jetson Xavier contain a vulnerability in camera firmware where a user can change input data after validation, which may lead to co denial of service and serious data corruption of all kernel components.
CVE-2021-37651	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation for `tf.raw_ops.FractionalAvgPoolGrad` can be tricked accessing data outside of bounds of heap allocated buffers. The [implementation] (https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/fractional_avg_pool_op.cc#L205) does not valid input tensor is non-empty. Thus, code constructs an empty `EigenDoubleMatrixMap` and then accesses this buffer with indices that are outside of the empty area. We patched the issue in GitHub commit 0f931751fb20f565c4e94aa6df58d54a003cdb30. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit o TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37658	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null p operations of type `tf.raw_ops.MatrixSetDiagV*`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/linalg/matrix_diag_op.cc) has incomplete valida the value of `k` is a valid tensor. We have check that this value is either a scalar or a vector, but there is no check for the number of elements. If this is an empty tensor, that accesses the first element of the tensor is wrong. We have patched the issue in GitHub commit ff8894044dfae5568ecbf2ed514c1a37dc394f1b. The fix will be inclu TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported r
CVE-2021-37697	tmerc-cogs are a collection of open source plugins for the Red Discord bot. A vulnerability has been found in the code that allows any user to access sensitive informati crafting a specific membership event message. Issue is patched in commit d63c49b4cfc30c795336e4fff08cba3795e0fcc0. As a workaround users may unload the Welc
CVE-2021-37656	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause undefined behavior via binding a reference to null p `tf.raw_ops.RaggedTensorToSparse`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/ragged_tensor_to_sparse_kernel.cc#L30) has a incomplete validation of the splits values: it does not check that they are in increasing order. We have patched the issue in GitHub commit 1071f554dbd09f7e101324d366eec5f4fe5a3ece. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4. TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-33762	Azure CycleCloud Elevation of Privilege Vulnerability
CVE-2021-34487	Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-26426	Windows User Account Profile Picture Elevation of Privilege Vulnerability
CVE-2021-38523	NETGEAR R6400 devices before 1.0.1.70 are affected by a stack-based buffer overflow by an authenticated user.
CVE-2021-37699	Next.js is an open source website development framework to be used with the React library. In affected versions specially encoded paths could be used when pages/_ statically generated allowing an open redirect to occur to an external site. In general, this redirect does not directly harm users although can allow for phishing attacks b redirecting to an attacker's domain from a trusted domain. We recommend everyone to upgrade regardless of whether you can reproduce the issue or not. The issue ha patched in release 11.1.0.
CVE-2021-38517	Certain NETGEAR devices are affected by out-of-bounds reads and writes. This affects R6400 before 1.0.1.70, RAX75 before 1.0.4.120, RAX80 before 1.0.4.120, and before 1.0.3.50.
CVE-2021-32826	Proxyee-Down is open source proxy software. An attacker being able to provide an extension script (eg: through a MiTM attack or by hosting a malicious extension) ma to run arbitrary commands on the system running Proxyee-Down. For more details including a PoC see the referenced GHSL-2021-053. As of the writing of this CVE th currently no patched version.
CVE-2021-38532	NETGEAR WAC104 devices before 1.0.4.15 are affected by incorrect configuration of security settings.

CVE Number	Description
CVE-2020-18454	Cross Site Request Forgery (CSRF) vulnerability in bycms v1.3 via admin.php/systems/index/module_id/70/group_id/1.html.
CVE-2021-34480	Scripting Engine Memory Corruption Vulnerability
CVE-2021-3046	An improper authentication vulnerability exists in Palo Alto Networks PAN-OS software that enables a SAML authenticated attacker to impersonate any other user in th GlobalProtect Portal and GlobalProtect Gateway when they are configured to use SAML authentication. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS PAN-OS 9.0 versions earlier than PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PAN-OS 9.1.9; PAN-OS 10.0 versions earlier than PAN-OS 10.0.5. PAN-OS 10.1 are not impacted.
CVE-2020-18457	Cross Site Request Forgery (CSRF) vulnerability exists in bycms v1.3.0 that can add an admin account via admin.php/ucenter/add.html.
CVE-2021-38525	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6200 l 1.1.00.36, D7000 before 1.0.1.70, EX6200v2 before 1.0.1.78, EX7000 before 1.0.1.78, EX8000 before 1.0.1.186, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6 1.0.0.42, R6050 before 1.0.1.18, R6080 before 1.0.0.42, R6120 before 1.0.0.46, R6220 before 1.1.0.80, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6700 befor R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 before 1.2.0.36, R7000 before 1.0.9.42, R7000P before 1.3 R7800 before 1.0.2.60, R8900 before 1.0.4.12, R9000 before 1.0.4.12, and XR500 before 2.3.2.40.
CVE-2021-38522	NETGEAR R6400 devices before 1.0.1.52 are affected by a stack-based buffer overflow by an authenticated user.
CVE-2021-34534	Windows MSHTML Platform Remote Code Execution Vulnerability
CVE-2021-3459	A privilege escalation vulnerability was reported in the MM1000 device configuration web server, which could allow privileged shell access and/or arbitrary privileged co be executed on the adapter.
CVE-2021-37028	There is a command injection vulnerability in the HG8045Q product. When the command-line interface is enabled, which is disabled by default, attackers with administr privilege could execute part of commands.
CVE-2021-1111	Bootloader contains a vulnerability in the NV3P server where any user with physical access through USB can trigger an incorrect bounds check, which may lead to buff overflow, resulting in limited information disclosure, limited data integrity, and denial of service across all components.
CVE-2021-0114	Unchecked return value in the firmware for some Intel(R) Processors may allow a privileged user to potentially enable an escalation of privilege via local access.
CVE-2021-37690	TensorFlow is an end-to-end open source platform for machine learning. In affected versions when running shape functions, some functions (such as `MutableHashTat produce extra output information in the form of a `ShapeAndType` struct. The shapes embedded in this struct are owned by an inference context that is cleaned up alm immediately; if the upstream code attempts to access this shape information, it can trigger a segfault. `ShapeRefiner` is mitigating this for normal output shapes by clon (and thus putting the newly created shape under ownership of an inference context that will not die), but we were not doing the same for shapes and types. This commi by doing similar logic on output shapes and types. We have patched the issue in GitHub commit ee119d4a498979525046fba1c3dd3f13a039fbb1. The fix will be include TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported r
CVE-2021-38520	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6400 before 1.0.1.52, R6400v2 before 1.0.4.84, R6700v3 before R6700v2 before 1.2.0.62, R6900v2 before 1.2.0.62, and R7000P before 1.3.2.124.
CVE-2021-3615	A vulnerability was reported in Lenovo Smart Camera X3, X5, and C2E that could allow code execution if a specific file exists on the attached SD card. This vulnerabilit same as CNVD-2021-45262.
CVE-2020-21066	An issue was discovered in Bento4 v1.5.1.0. There is a heap-buffer-overflow in AP4_Dec3Atom::AP4_Dec3Atom at Ap4Dec3Atom.cpp, leading to a denial of service (p crash), as demonstrated by mp42aac.
CVE-2020-4992	IBM DataPower Gateway 2018.4.1.0 through 2018.4.1.16 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorize transmitted from a user that the website trusts. IBM X-Force ID: 192737.
CVE-2021-29880	IBM QRadar SIEM 7.4.3 GA - 7.4.3 Fix Pack 1 when using domains or multi-tenancy could be vulnerable to information disclosure between tenants by routing SIEM da incorrect domain. IBM X-Force ID: 206979.
CVE-2021-32067	The MiCollab Client Service component in Mitel MiCollab before 9.3 could allow an attacker to view sensitive system information through an HTTP response due to insu output sanitization.

CVE Number	Description
CVE-2020-28846	Cross Site Request Forgery (CSRF) vulnerability exists in SeaCMS 10.7 in admin_manager.php, which could let a malicious user add an admin account.
CVE-2021-32072	The MiCollab Client Service component in Mitel MiCollab before 9.3 could allow an attacker to get source code information (disclosing sensitive application data) due to insufficient output sanitization. A successful exploit could allow an attacker to view source code methods.
CVE-2021-27402	The SAS Admin portal of Mitel MiCollab before 9.2 FP2 could allow an unauthenticated attacker to access (view and modify) user data by injecting arbitrary directory pa improper URL validation, aka Directory Traversal.
CVE-2021-0580	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker with no addi execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187231637
CVE-2021-37709	Shopware is an open source eCommerce platform. Versions prior to 6.4.3.1 contain a vulnerability involving an insecure direct object reference of log files of the Import feature. Version 6.4.3.1 contains a patch. As workarounds for older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin.
CVE-2021-0579	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker with no addi execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187231636
CVE-2020-21363	An arbitrary file deletion vulnerability exists within Maccms10.
CVE-2021-22933	A vulnerability in Pulse Connect Secure before 9.1R12 could allow an authenticated administrator to perform an arbitrary file delete via a maliciously crafted web reque
CVE-2021-37707	Shopware is an open source eCommerce platform. Versions prior to 6.4.3.1 contain a vulnerability that allows manipulation of product reviews via API. Version 6.4.3.1 patch. As workarounds for older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin.
CVE-2020-25562	In SapphireIMS 5.0, there is no CSRF token present in the entire application. This can lead to CSRF vulnerabilities in critical application forms like account resent.
CVE-2021-0582	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker with no addi execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187149601
CVE-2021-0581	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker with no addi execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187231638
CVE-2017-16631	In SapphireIMS 4097_1, a guest user is able to change the password of an administrative user by utilizing an Insecure Direct Object Reference (IDOR) in the "Account Reset" functionality.
CVE-2021-29987	After requesting multiple permissions, and closing the first permission panel, subsequent permission panels will be displayed in a different position but still record a click default location, making it possible to trick a user into accepting a permission they did not want to. *This bug only affects Firefox on Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox < 91 and Thunderbird < 91.
CVE-2021-37700	@github/paste-markdown is an npm package for pasting markdown objects. A self Cross-Site Scripting vulnerability exists in the @github/paste-markdown before versi the clipboard data contains the string `<table>`, a **div** is dynamically created, and the clipboard content is copied into its **innerHTML** property without any sanitiza resulting in improper execution of JavaScript in the browser of the victim (the user who pasted the code). Users directed to copy text from a malicious website and paste pages that utilize this library are affected. This is fixed in version 0.3.4. Refer the to the referenced GitHub Advisory for more details including an example exploit.
CVE-2021-29982	Due to incorrect JIT optimization, we incorrectly interpreted data from the wrong type of object, resulting in the potential leak of a single bit of memory. This vulnerability Firefox < 91 and Thunderbird < 91.
CVE-2021-29983	Firefox for Android could get stuck in fullscreen mode and not exit it even after normal interactions that should cause it to exit. *Note: This issue only affected Firefox for Other operating systems are unaffected.*. This vulnerability affects Firefox < 91.
CVE-2021-0578	In wifi driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure to a proximal attacker with no addi execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-187161772
CVE-2021-39247	Zint Barcode Generator before 2.10.0 has a one-byte buffer over-read, related to is_last_single_ascii in code1.c, and rs_encode_uint in reedsol.c.

CVE Number	Description
CVE-2021-31731	A directory traversal issue in KiteCMS 1.1.1 allows remote administrators to overwrite arbitrary files via ../ in the path parameter to index.php/admin/Template/fileedit, w code in the html parameter.
CVE-2021-0009	Out-of-bounds read in the firmware for Intel(R) Ethernet Adapters 800 Series Controllers and associated adapters before version 1.5.3.0 may allow an unauthenticated potentially enable denial of service via adjacent access.
CVE-2021-34641	The SEOPress WordPress plugin is vulnerable to Stored Cross-Site-Scripting via the processPut function found in the ~/src/Actions/Api/TitleDescriptionMeta.php file wl authenticated attackers to inject arbitrary web scripts, in versions 5.0.0 - 5.0.3.
CVE-2021-3573	A use-after-free in function hci_sock_bound_ioctl() of the Linux kernel HCI subsystem was found in the way user calls ioct HCIUNBLOCKADDR or other way triggers ra condition of the call hci_unregister_dev() together with one of the calls hci_sock_blacklist_add(), hci_sock_blacklist_del(), hci_get_conn_info(), hci_get_auth_info(). A p local user could use this flaw to crash the system or escalate their privileges on the system. This flaw affects the Linux kernel versions prior to 5.13-rc5.
CVE-2021-38538	Certain NETGEAR devices are affected by stored XSS. This affects D7800 before 1.0.1.56, R7800 before 1.0.2.68, R8900 before 1.0.4.26, R9000 before 1.0.4.26, RA before 1.0.0.78, RBK20 before 2.3.5.26, RBR20 before 2.3.5.26, RBS20 before 2.3.5.26, RBK40 before 2.3.5.30, RBR40 before 2.3.5.30, RBS40 before 2.3.5.30, RBK 2.3.5.30, RBR50 before 2.3.5.30, RBS50 before 2.3.5.30, and XR500 before 2.3.2.56.
CVE-2021-38539	Certain NETGEAR devices are affected by privilege escalation. This affects D8500 before 1.0.3.44, R6400v2 before 1.0.2.66, R6700 before 1.0.2.6, R6700v3 before 1. R6900 before 1.0.2.4, R6900P before 1.3.2.126, R7000 before 1.0.9.42, R7000P before 1.3.2.126, R7100LG before 1.0.0.50, R7300DST before 1.0.0.70, R7900 befor R8300 before 1.0.2.130, and R8500 before 1.0.2.130.
CVE-2021-38519	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6250 before 1.0.4.36, R6300v2 before 1.0.4.36, R6400 before 1. R6400v2 before 1.0.2.66, R6700v3 before 1.0.2.66, R6700 before 1.0.2.8, R6900 before 1.0.2.8, R7000 before 1.0.9.88, R6900P before 1.3.2.132, R7100LG before 1. R7900 before 1.0.3.10, R8000 before 1.0.4.46, R7900P before 1.4.1.50, R8000P before 1.4.1.50, and RAX80 before 1.0.1.40.
CVE-2021-34658	The Simple Popup Newsletter WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of $_SERVER['PHP_SELF'] in the ~/simple-popup-news file which allows attackers to inject arbitrary web scripts, in versions up to and including 1.4.7.
CVE-2021-24536	The Custom Login Redirect WordPress plugin through 1.0.0 does not have CSRF check in place when saving its settings, and do not sanitise or escape user input befo outputting them back in the page, leading to a Stored Cross-Site Scripting issue
CVE-2021-34649	The Simple Behance Portfolio WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `dark` parameter in the ~/titan-framework/iframe-font-preview.ph which allows attackers to inject arbitrary web scripts, in versions up to and including 0.2.
CVE-2021-34657	The 2TypoFR WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the text function found in the ~/vendor/Org_Heigl/Hyphenator/index.php file which al attackers to inject arbitrary web scripts, in versions up to and including 0.11.
CVE-2021-34666	The Add Sidebar WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the add parameter in the ~/wp_sidebarMenu.php file which allows attackers to inj arbitrary web scripts, in versions up to and including 2.0.0.
CVE-2021-38757	Persistent cross-site scripting (XSS) in Hospital Management System targeted towards web admin through contact.php.
CVE-2021-36790	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 allows XSS.
CVE-2021-34665	The WP SEO Tags WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the saq_txt_the_filter parameter in the ~/wp-seo-tags.php file which allows atta inject arbitrary web scripts, in versions up to and including 2.2.7.
CVE-2021-34664	The Moova for WooCommerce WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the lat parameter in the ~/Checkout/Checkout.php file which allows to inject arbitrary web scripts, in versions up to and including 3.5.
CVE-2021-34663	The jQuery Tagline Rotator WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of $_SERVER['PHP_SELF'] in the ~/jquery-tagline-rotator.p which allows attackers to inject arbitrary web scripts, in versions up to and including 0.1.5.
CVE-2021-34659	The Plugmatter Pricing Table Lite WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `email` parameter in the ~/license.php file which allows attac inject arbitrary web scripts, in versions up to and including 1.0.32.
CVE-2021-38756	Persistent cross-site scripting (XSS) in Hospital Management System targeted towards web admin through prescribe.php.

CVE Number	Description
CVE-2021-34642	The Smart Email Alerts WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the api_key in the ~/views/settings.php file which allows attackers to inject web scripts, in versions up to and including 1.0.10.
CVE-2020-18699	Cross Site Scripting (XSS) in Lin-CMS-Flask v0.1.1 allows remote attackers to execute arbitrary code by entering scripts in the the 'Username' parameter of the in comp 'app/api/cms/user.py'.
CVE-2021-24535	The Light Messages WordPress plugin through 1.0 is lacking CSRF check when updating it's settings, and is not sanitising its Message Content in them (even with the unfiltered_html disallowed). As a result, an attacker could make a logged in admin update the settings to arbitrary values, and set a Cross-Site Scripting payload in the Content. Depending on the options set, the XSS payload can be triggered either in the backend only (in the plugin's settings), or both frontend and backend.
CVE-2021-38709	In ocProducts Composr CMS before 10.0.38, an attacker can inject JavaScript via the staff_messaging messaging system for XSS.
CVE-2021-34653	The WP Fountain WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of $_SERVER['PHP_SELF'] in the ~/wp-fountain.php file which allow to inject arbitrary web scripts, in versions up to and including 1.5.9.
CVE-2021-34654	The Custom Post Type Relations WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the cptr[name] parameter found in the ~/pages/admin-page.php allows attackers to inject arbitrary web scripts, in versions up to and including 1.0.
CVE-2021-24362	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery WordPress plugin before 1.5.75 did not ensure that uploaded SVG files added to a gallery do not contain content. As a result, users allowed to add images to gallery can upload an SVG file containing JavaScript code, which will be executed when accessing the image direc the /wp-content/uploads/photo-gallery/ folder), leading to a Cross-Site Scripting (XSS) issue
CVE-2021-34643	The Skaut bazar WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of $_SERVER['PHP_SELF'] in the ~/skaut-bazar.php file which allows to inject arbitrary web scripts, in versions up to and including 1.3.2.
CVE-2021-24410	The తెలుగు బైబిల్ వచనములు WordPress plugin through 1.0 is lacking any CSRF check when saving its settings and verses, and do not sanitise or escape them when them back in the page. This could allow attackers to make a logged in admin change the settings, as well as add malicious verses containing JavaScript code in them, Stored XSS issues
CVE-2021-24411	The Social Tape WordPress plugin through 1.0 does not have CSRF checks in place when saving its settings, and do not sanitise or escape them before outputting the the page, leading to a stored Cross-Site Scripting issue via a CSRF attack
CVE-2021-24466	The Verse-O-Matic WordPress plugin through 4.1.1 does not have any CSRF checks in place, allowing attackers to make logged in administrators do unwanted actions add/edit/delete arbitrary verses and change the settings. Due to the lack of sanitisation in the settings and verses, this could also lead to Stored Cross-Site Scripting iss
CVE-2021-34656	The 2Way VideoCalls and Random Chat - HTML5 Webcam Videochat WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the `vws_notice` function fo ~/inc/requirements.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 5.2.7.
CVE-2021-34655	The WP Songbook WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the url parameter found in the ~/inc/class.ajax.php file which allows attackers to arbitrary web scripts, in versions up to and including 2.0.11.
CVE-2021-34644	The Multiplayer Games WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of $_SERVER['PHP_SELF'] in the ~/multiplayergames.php file allows attackers to inject arbitrary web scripts, in versions up to and including 3.7.
CVE-2021-22936	A vulnerability in Pulse Connect Secure before 9.1R12 could allow a threat actor to perform a cross-site script attack against an authenticated administrator via an unsa web parameter.
CVE-2021-32827	MockServer is open source software which enables easy mocking of any system you integrate with via HTTP or HTTPS. An attacker that can trick a victim into visiting site while running MockServer locally, will be able to run arbitrary code on the MockServer machine. With an overly broad default CORS configuration MockServer allow to send cross-site requests. Additionally, MockServer allows you to create dynamic expectations using Javascript or Velocity templates. Both engines may allow an atta execute arbitrary code on-behalf of MockServer. By combining these two issues (Overly broad CORS configuration + Script injection), an attacker could serve a malicio that if a developer running MockServer visits it, they will get compromised. For more details including a PoC see the referenced GHSL-2021-059.
CVE-2021-34667	The Calendar_plugin WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of `$_SERVER['PHP_SELF']` in the ~/calendar.php file which allo attackers to inject arbitrary web scripts, in versions up to and including 1.0.
CVE-2020-18702	Cross Site Scripting (XSS) in Quokka v0.4.0 allows remote attackers to execute arbitrary code via the 'Username' parameter in the component 'quokka/admin/actions.p
CVE-2021-38315	The SP Project & Document Manager WordPress plugin is vulnerable to attribute-based Reflected Cross-Site Scripting via the from and to parameters in the ~/function which allows attackers to inject arbitrary web scripts, in versions up to and including 4.25.

CVE Number	Description
CVE-2021-34651	The Scribble Maps WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the map parameter in the ~/includes/admin.php file which allows attackers to in arbitrary web scripts, in versions up to and including 1.2.
CVE-2021-29313	Cross Site Scripting (XSS) vulnerability exists in SeaCMS 12.6 via the (1) v_company and (2) v_tvs parameters in /admin_video.php,
CVE-2020-23341	A reflected cross site scripting (XSS) vulnerability in the /header.tmpl.php component of ATutor 2.2.4 allows attackers to execute arbitrary web scripts or HTML via a cra payload.
CVE-2021-3458	The Motorola MM1000 device configuration portal can be accessed without authentication, which could allow adapter settings to be modified.
CVE-2021-34652	The Media Usage WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the id parameter in the ~/mmu_admin.php file which allows attackers to inject ar scripts, in versions up to and including 0.0.4.
CVE-2021-34640	The Securimage-WP-Fixed WordPress plugin is vulnerable to Reflected Cross-Site Scripting due to the use of $_SERVER['PHP_SELF'] in the ~/securimage-wp.php fil allows attackers to inject arbitrary web scripts, in versions up to and including 3.5.4.
CVE-2021-38087	Reflected cross-site scripting (XSS) was possible on the login page in Acronis Cyber Protect 15 prior to build 27009.
CVE-2021-38702	Cyberoam NetGenie C0101B1-20141120-NG11VO devices through 2021-08-14 allow tweb/ft.php?u=[XSS] attacks.
CVE-2020-18445	Cross Site Scripting (XSS) vulnerability exists in YUNUCMS 1.1.9 via the upurl function in Page.php.
CVE-2021-39248	Open edX through Lilac.1 allows XSS in common/static/common/js/discussion/utils.js via crafted LaTeX content within a discussion.
CVE-2021-39249	Invision Community (aka IPS Community Suite or IP-Board) before 4.6.5.1 allows reflected XSS because the filenames of uploaded files become predictable through a attack against the PHP mt_rand function.
CVE-2021-38521	Certain NETGEAR devices are affected by command injection by an authenticated user. This affects R6400 before 1.0.1.50, R7900P before 1.4.1.50, R8000P before 1 RAX75 before 1.0.1.62, and RAX80 before 1.0.1.62.
CVE-2021-37352	An open redirect vulnerability exists in Nagios XI before version 5.8.5 that could lead to spoofing. To exploit the vulnerability, an attacker could send a link that has a sp crafted URL and convince the user to click the link.
CVE-2021-22098	UAA server versions prior to 75.4.0 are vulnerable to an open redirect vulnerability. A malicious user can exploit the open redirect vulnerability by social engineering lea take over of victims' accounts in certain cases along with redirection of UAA users to a malicious sites.
CVE-2021-38583	openBaraza HCM 3.1.6 does not properly neutralize user-controllable input, which allows reflected cross-site scripting (XSS) on multiple pages: hr/subscription.jsp and hr/application.jsp and and hr/index.jsp (with view= and data=).
CVE-2021-38619	openBaraza HCM 3.1.6 does not properly neutralize user-controllable input: an unauthenticated remote attacker can conduct a stored cross-site scripting (XSS) attack administrative user from hr/subscription.jsp and hr/application.jsp and and hr/index.jsp (with view=).
CVE-2021-27401	The Join Meeting page of Mitel MiCollab Web Client before 9.2 FP2 could allow an attacker to access (view and modify) user data by executing arbitrary code due to in input validation, aka Cross-Site Scripting (XSS).
CVE-2021-21599	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.1.x contain an OS command injection vulnerability. This may allow a user with ISI_PRIV_LOGIN_SSH or ISI_PRIV_LOGIN_CONSOLE to escalate privileges and escape the compliance guarantees. This only impacts Smartlock WORM compliance mode clusters as a critica vulnerability and Dell recommends to update/upgrade at the earliest opportunity.
CVE-2021-21595	Dell EMC PowerScale OneFS versions 8.2.x - 9.1.1.x contain an improper neutralization of special elements used in an OS command. This vulnerability could allow the compadmin user to elevate privileges. This only impacts Smartlock WORM compliance mode clusters as a critical vulnerability and Dell recommends to update/upgrade earliest opportunity.

CVE Number	Description
CVE-2021-26430	Azure Sphere Denial of Service Vulnerability
CVE-2021-38548	JBL Go 2 devices through 2021-08-09 allow remote attackers to recover speech signals from an LED on the device, via a telescope and an electro-optical sensor, aka "Glowworm" attack. The power indicator LED of the speakers is connected directly to the power line, as a result, the intensity of a device's power indicator LED is corre power consumption. The sound played by the speakers affects their power consumption and as a result is also correlative to the light intensity of the LEDs. By analyzin measurements obtained from an electro-optical sensor directed at the power indicator LEDs of the speakers, we can recover the sound played by them.
CVE-2021-3048	Certain invalid URL entries contained in an External Dynamic List (EDL) cause the Device Server daemon (devsrvr) to stop responding. This condition causes subsequ commits on the firewall to fail and prevents administrators from performing commits and configuration changes even though the firewall remains otherwise functional. If then restarts, it results in a denial-of-service (DoS) condition and the firewall stops processing traffic. This issue impacts: PAN-OS 9.0 versions earlier than PAN-OS 9.0 OS 9.1 versions earlier than PAN-OS 9.1.9; PAN-OS 10.0 versions earlier than PAN-OS 10.0.5. PAN-OS 8.1 and PAN-OS 10.1 versions are not impacted.
CVE-2021-38549	MIRACASE MHUB500 USB splitters through 2021-08-09, in certain specific use cases in which the device supplies power to audio-output equipment, allow remote atta recover speech signals from an LED on the device, via a telescope and an electro-optical sensor, aka a "Glowworm" attack. We assume that the USB splitter supplies some speakers. The power indicator LED of the USB splitter is connected directly to the power line, as a result, the intensity of the USB splitter's power indicator LED is correlative to its power consumption. The sound played by the connected speakers affects the USB splitter's power consumption and as a result is also correlative to th intensity of the LED. By analyzing measurements obtained from an electro-optical sensor directed at the power indicator LED of the USB splitter, we can recover the so by the connected speakers.
CVE-2021-38546	CREATIVE Pebble devices through 2021-08-09 allow remote attackers to recover speech signals from an LED on the device, via a telescope and an electro-optical ser "Glowworm" attack. The power indicator LED of the speakers is connected directly to the power line, as a result, the intensity of a device's power indicator LED is corre power consumption. The sound played by the speakers affects their power consumption and as a result is also correlative to the light intensity of the LEDs. By analyzin measurements obtained from an electro-optical sensor directed at the power indicator LEDs of the speakers, we can recover the sound played by them.
CVE-2021-38547	Logitech Z120 and S120 speakers through 2021-08-09 allow remote attackers to recover speech signals from an LED on the device, via a telescope and an electro-opt sensor, aka a "Glowworm" attack. The power indicator LED of the speakers is connected directly to the power line, as a result, the intensity of a device's power indicato correlative to the power consumption. The sound played by the speakers affects their power consumption and as a result is also correlative to the light intensity of the L analyzing measurements obtained from an electro-optical sensor directed at the power indicator LEDs of the speakers, we can recover the sound played by them.
CVE-2021-38545	Raspberry Pi 3 B+ and 4 B devices through 2021-08-09, in certain specific use cases in which the device supplies power to audio-output equipment, allow remote attac recover speech signals from an LED on the device, via a telescope and an electro-optical sensor, aka a "Glowworm" attack. We assume that the Raspberry Pi supplies some speakers. The power indicator LED of the Raspberry Pi is connected directly to the power line, as a result, the intensity of a device's power indicator LED is corre the power consumption. The sound played by the speakers affects the Raspberry Pi's power consumption and as a result is also correlative to the light intensity of the L analyzing measurements obtained from an electro-optical sensor directed at the power indicator LED of the Raspberry Pi, we can recover the sound played by the spea
CVE-2021-38544	Sony SRS-XB33 and SRS-XB43 devices through 2021-08-09 allow remote attackers to recover speech signals from an LED on the device, via a telescope and an elec sensor, aka a "Glowworm" attack. The power indicator LED of the speakers is connected directly to the power line, as a result, the intensity of a device's power indicato correlative to the power consumption. The sound played by the speakers affects their power consumption and as a result is also correlative to the light intensity of the L analyzing measurements obtained from an electro-optical sensor directed at the power indicator LEDs of the speakers, we can recover the sound played by them.
CVE-2021-38543	TP-Link UE330 USB splitter devices through 2021-08-09, in certain specific use cases in which the device supplies power to audio-output equipment, allow remote atta recover speech signals from an LED on the device, via a telescope and an electro-optical sensor, aka a "Glowworm" attack. We assume that the USB splitter supplies some speakers. The power indicator LED of the USB splitter is connected directly to the power line, as a result, the intensity of the USB splitter's power indicator LED is correlative to its power consumption. The sound played by the connected speakers affects the USB splitter's power consumption and as a result is also correlative to th intensity of the LED. By analyzing measurements obtained from an electro-optical sensor directed at the power indicator LED of the USB splitter, we can recover the so by the connected speakers.
CVE-2020-15955	In s/qmail through 4.0.07, an active MitM can inject arbitrary plaintext commands into a STARTTLS encrypted session between an SMTP client and s/qmail. This allows messages and user credentials to be sent to the MitM attacker.
CVE-2021-38597	wolfSSL before 4.8.1 incorrectly skips OCSP verification in certain situations of irrelevant response data that contains the NoCheck extension.
CVE-2021-23421	All versions of package merge-change are vulnerable to Prototype Pollution via the utils.set function.
CVE-2021-0642	In onResume of VoicemailSettingsFragment.java, there is a possible way to retrieve a trackable identifier without permissions due to a missing permission check. This to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-Android-8.1 Android-9Android ID: A-185126149
CVE-2021-37636	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of `tf.raw_ops.SparseDenseCwiseDiv` is vulnerable to by 0 error. The [implementation] (https://github.com/tensorflow/tensorflow/blob/a1bc56203f21a5a4995311825ffaba7a670d7747/tensorflow/core/kernels/sparse_dense_binary_op_shared.cc#L56) uses class for all binary operations but fails to treat the division by 0 case separately. We have patched the issue in GitHub commit d9204be9f49520cdaaeb2541d1dc5187b The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affect in supported range.
CVE-2021-38590	In cPanel before 96.0.8, weak permissions on web stats can lead to information disclosure (SEC-584).

CVE Number	Description
CVE-2021-1112	NVIDIA Linux kernel distributions contain a vulnerability in nvmap, where a null pointer dereference may lead to complete denial of service.
CVE-2021-32440	The Media_RewriteODFrame function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box comman
CVE-2021-32438	The gf_media_export_filters function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command
CVE-2021-32437	The gf_hinter_finalize function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.
CVE-2021-0012	Use after free in some Intel(R) Graphics Driver before version 27.20.100.8336, 15.45.33.5164, and 15.40.47.5166 may allow an authenticated user to potentially enable service via local access.
CVE-2021-0003	Improper conditions check in some Intel(R) Ethernet Controllers 800 series Linux drivers before version 1.4.11 may allow an authenticated user to potentially enable inf disclosure via local access.
CVE-2021-0641	In getAvailableSubscriptionInfoList of SubscriptionController.java, there is a possible disclosure of unique identifiers due to a missing permission check. This could lead information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 A Android-11Android ID: A-185235454
CVE-2021-37640	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of `tf.raw_ops.SparseReshape` can be made to trigge integral division by 0 exception. The [implementation] (https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/reshape_util.cc#L176-L181) calls the reshaping whenever there is at least an index in the input but does not check that shape of the input or the target shape have both a non-zero number of elements. The [reshape (https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/reshape_util.cc#L40-L78) blindly divides by the of the target shape. Hence, if this is not checked, code will result in a division by 0. We have patched the issue in GitHub commit 4923de56ec94fff7770df259ab7f2288a The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1 as this is the other affected version.
CVE-2021-0639	In multiple functions of libl3oemcrypto.cpp, there is a possible weakness in the existing obfuscation mechanism due to the way sensitive data is handled. This could lea information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: 190724551
CVE-2021-23423	This affects the package bikeshed before 3.0.0. This can occur when an untrusted source file containing include, include-code or include-raw block is processed. The c arbitrary files could be disclosed in the HTML output.
CVE-2021-37692	TensorFlow is an end-to-end open source platform for machine learning. In affected versions under certain conditions, Go code can trigger a segfault in string deallocat string tensors, `C.TF_TString_Dealloc` is called during garbage collection within a finalizer function. However, tensor structure isn't checked until encoding to avoid a pe penalty. The current method for dealloc assumes that encoding succeeded, but segfaults when a string tensor is garbage collected whose encoding failed (e.g., due to mismatched dimensions). To fix this, the call to set the finalizer function is deferred until `NewTensor` returns and, if encoding failed for a string tensor, deallocs are det based on bytes written. We have patched the issue in GitHub commit 8721ba96e5760c229217b594f6d2ba332beedf22. The fix will be included in TensorFlow 2.6.0. W cherrypick this commit on TensorFlow 2.5.1, which is the other affected version.
CVE-2021-37691	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can craft a TFLite model that would trigger a division by zero e LSH [implementation](https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/lsh_projection.cc#L118). We patched the issue in GitHub commit 0575b640091680cfb70f4dd93e70658de43b94f9. The fix will be included in TensorFlow 2.6.0. We will also cherrypick thiscommit o TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37687	TensorFlow is an end-to-end open source platform for machine learning. In affected versions TFLite's [`GatherNd` implementation] (https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/gather_nd.cc#L124) does not support negative in there are no checks for this situation. Hence, an attacker can read arbitrary data from the heap by carefully crafting a model with negative values in `indices`. Similar iss in [`Gather` implementation](https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/gather.cc). We have p issue in GitHub commits bb6a0383ed553c286f87ca88c207f6774d5c4a8f and eb921122119a6b6e470ee98b89e65d721663179d. The fix will be included in TensorFlow will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37685	TensorFlow is an end-to-end open source platform for machine learning. In affected versions TFLite's [`expand_dims.cc`] (https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/expand_dims.cc#L36-L50) contains a vulnerabilit allows reading one element outside of bounds of heap allocated data. If `axis` is a large negative value (e.g., `-100000`), then after the first `if` it would still be negative. following the `if` statement will pass and the `for` loop would read one element before the start of `input_dims.data` (when `i = 0`). We have patched the issue in GitHub d94ffe08a65400f898241c0374e9edc6fa8ed257. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4. TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37684	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementations of pooling in TFLite are vulnerable to division by 0 er there are no checks for divisors not being 0. We have patched the issue in GitHub commit [dfa22b348b70bb89d6d6ec0ff53973bacb4f4695] (https://github.com/tensorflow/tensorflow/commit/dfa22b348b70bb89d6d6ec0ff53973bacb4f4695). The fix will be included in TensorFlow 2.6.0. We will also cherrypick on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-37683	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of division in TFLite is [vulnerable to a division by 0 er (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/div.cc). There is no check that the divisor tensor c contain zero elements. We have patched the issue in GitHub commit 1e206baedf8bef0334cca3eb92bab134ef525a28. The fix will be included in TensorFlow 2.6.0. We cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37677	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the shape inference code for `tf.raw_ops.Dequantize` has a vulnerability t trigger a denial of service via a segfault if an attacker provides invalid arguments. The shape inference [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/ops/array_ops.cc#L2999-L3014) uses `axis` to select be different values for `minmax_rank` which is then used to retrieve tensor dimensions. However, code assumes that `axis` can be either `-1` or a value greater than `-1`, validation for the other values. We have patched the issue in GitHub commit da857cfa0fde8f79ad0afdbc94e88b5d4bbec764. The fix will be included in TensorFlow 2.6 also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37674	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can trigger a denial of service via a segmentation fault in `tf.raw_ops.MaxPoolGrad` caused by missing validation. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/maxpooling_op.cc) misses some validation for t `orig_input` and `orig_output` tensors. The fixes for CVE-2021-29579 were incomplete. We have patched the issue in GitHub commit 136b51f10903e044308cf77117c0ed9871350475. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2. TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37673	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.MapStage`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/map_stage_op.cc#L513) does not check that th input is a valid non-empty tensor. We have patched the issue in GitHub commit d7de67733925de196ec8863a33445b73f9562d1d. The fix will be included in TensorFlo We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37672	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can read from outside of bounds of heap allocated data by se specially crafted illegal arguments to `tf.raw_ops.SdcaOptimizerV2`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/sdca_internal.cc#L320-L353) does not check tha length of `example_labels` is the same as the number of examples. We have patched the issue in GitHub commit a4e138660270e7599793fa438cd7b2fc2ce215a6. The included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in range.
CVE-2021-3707	D-Link router DSL-2750U with firmware vME1.16 or prior versions is vulnerable to unauthorized configuration modification. An unauthenticated attacker on the local net exploit this, with CVE-2021-3708, to execute any OS commands on the vulnerable device.
CVE-2021-37670	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can read from outside of bounds of heap allocated data by se specially crafted illegal arguments to `tf.raw_ops.UpperBound`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/searchsorted_op.cc#L85-L104) does not validat of `sorted_input` argument. A similar issue occurs in `tf.raw_ops.LowerBound`. We have patched the issue in GitHub commit 42459e4273c2e47a3232cc16c4f4fff3b3a fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected a supported range.
CVE-2021-37669	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause denial of service in applications serving models usi `tf.raw_ops.NonMaxSuppressionV5` by triggering a division by 0. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/image/non_max_suppression_op.cc#L170-L271 user controlled argument to resize a `std::vector`. However, as `std::vector::resize` takes the size argument as a `size_t` and `output_size` is an `int`, there is an implici conversion to unsigned. If the attacker supplies a negative value, this conversion results in a crash. A similar issue occurs in `CombinedNonMaxSuppression`. We have the issue in GitHub commit 3a7362750d5c372420aa8f0caf7bf5b5c3d0f52d and commit [b5cdbf12ffcaaffecf98f22a6be5a64bb96e4f58. The fix will be included in Tenso 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37668	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause denial of service in applications serving models usi `tf.raw_ops.UnravelIndex` by triggering a division by 0. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/unravel_index_op.cc#L36) does not check that t subsumed by `dims` is not empty. Hence, if one element of `dims` is 0, the implementation does a division by 0. We have patched the issue in GitHub commit a776040a5e7ebf76eeb7eb923bf1ae417dd4d233. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2. TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-34532	ASP.NET Core and Visual Studio Information Disclosure Vulnerability
CVE-2021-37686	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the strided slice implementation in TFLite has a logic bug which can allow attacker to trigger an infinite loop. This arises from newly introduced support for [ellipsis in axis definition] (https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/tensorflow/lite/kernels/strided_slice.cc#L103-L122). An attacker can craf such that `ellipsis_end_idx` is smaller than `i` (e.g., always negative). In this case, the inner loop does not increase `i` and the `continue` statement causes execution to the preincrement at the end of the outer loop. We have patched the issue in GitHub commit dfa22b348b70bb89d6d6ec0ff53973bacb4f4695. TensorFlow 2.6.0 is the or version.
CVE-2021-37680	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of fully connected layers in TFLite is [vulnerable to a d zero error](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/fully_connected.cc#L226). We have pa issue in GitHub commit 718721986aa137691ee23f03638867151f74935f. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlo TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-37675	TensorFlow is an end-to-end open source platform for machine learning. In affected versions most implementations of convolution operators in TensorFlow are affected division by 0 vulnerability where an attacker can trigger a denial of service via a crash. The shape inference [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/framework/common_shape_fns.cc#L577) is missing sev validations before doing divisions and modulo operations. We have patched the issue in GitHub commit 8a793b5d7f59e37ac7f3cd0954a750a2fe76bad4. The fix will be in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supporte
CVE-2021-37661	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause a denial of service in `boosted_trees_create_quantile_stream_resource` by using negative arguments. The [implementation] (https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/boosted_trees/quantile_ops.cc#L96) does not v that `num_streams` only contains non-negative numbers. In turn, [this results in using this value to allocate memory] (https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/boosted_trees/quantiles/quantile_stream_resou L40). However, `reserve` receives an unsigned integer so there is an implicit conversion from a negative value to a large positive unsigned. This results in a crash from standard library. We have patched the issue in GitHub commit 8a84f7a2b5a2b27ecf88d25bad9ac777cd2f7992. The fix will be included in TensorFlow 2.6.0. We will als cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37646	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of `tf.raw_ops.StringNGrams` is vulnerable to an integ issue caused by converting a signed integer value to an unsigned one and then allocating memory based on this value. The [implementation] (https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/string_ngrams_op.cc#L184) calls `reserve` on a with a value that sometimes can be negative if user supplies negative `ngram_widths`. The `reserve` method calls `TF_TString_Reserve` which has an `unsigned long` for the size of the buffer. Hence, the implicit conversion transforms the negative value to a large integer. We have patched the issue in GitHub commit c283e542a3f422420cfdb332414543b62fc4e4a5. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4 TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37645	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of `tf.raw_ops.QuantizeAndDequantizeV4Grad` is vulr an integer overflow issue caused by converting a signed integer value to an unsigned one and then allocating memory based on this value. The [implementation] (https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/quantize_and_dequantize_op.cc#L126) uses the value as the size argument to `absl::InlinedVector` constructor. But, the constructor uses an unsigned type for the argument, so the implicit conversion transforms the n value to a large integer. We have patched the issue in GitHub commit 96f364a1ca3009f98980021c4b32be5fdcca33a1. The fix will be included in TensorFlow 2.6.0. We cherrypick this commit on TensorFlow 2.5.1, and TensorFlow 2.4.3, as these are also affected and still in supported range.
CVE-2021-24445	The My Site Audit WordPress plugin through 1.2.4 does not sanitise or escape the Audit Name field when creating an audit, allowing high privilege users to set JavaScr payloads in them, even when he unfiltered_html capability is disallowed, leading to an authenticated Stored Cross-Site Scripting issue
CVE-2021-37644	TensorFlow is an end-to-end open source platform for machine learning. In affected versions providing a negative element to `num_elements` list argument of `tf.raw_ops.TensorListReserve` causes the runtime to abort the process due to reallocating a `std::vector` to have a negative number of elements. The [implementation (https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/list_kernels.cc#L312) calls `std::vector.resize()` v new size controlled by input given by the user, without checking that this input is valid. We have patched the issue in GitHub commit 8a6e874437670045e6c7dc6154c7412b4a2135e2. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2 TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37660	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can cause a floating point exception by calling inplace operati crafted arguments that would result in a division by 0. The [implementation] (https://github.com/tensorflow/tensorflow/blob/84d053187cb80d975ef2b9684d4b61981bca0c41/tensorflow/core/kernels/inplace_ops.cc#L283) has a logic error: it shoul processing if `x` and `v` are empty but the code uses `||` instead of `&&`. We have patched the issue in GitHub commit e86605c0a336c088b638da02135ea6f9f675361 will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and supported range.
CVE-2021-37653	TensorFlow is an end-to-end open source platform for machine learning. In affected versions an attacker can trigger a crash via a floating point exception in `tf.raw_ops.ResourceGather`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/tensorflow/core/kernels/resource_variable_ops.cc#L725-L731) compute of a value, `batch_size`, and then divides by it without checking that this value is not 0. We have patched the issue in GitHub commit ac117ee8a8ea57b73d34665cdf00ef3303bc0b11. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4 TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-37642	TensorFlow is an end-to-end open source platform for machine learning. In affected versions the implementation of `tf.raw_ops.ResourceScatterDiv` is vulnerable to a 0 error. The [implementation] (https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/tensorflow/core/kernels/resource_variable_ops.cc#L865) uses a commo all binary operations but fails to treat the division by 0 case separately. We have patched the issue in GitHub commit 4aacb30888638da75023e6601149415b39763d76 will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and supported range.
CVE-2021-0584	In verifyBufferObject of Parcel.cpp, there is a possible out of bounds read due to an improper input validation. This could lead to local information disclosure with no ad execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-1792
CVE-2021-36938	Windows Cryptographic Primitives Library Information Disclosure Vulnerability
CVE-2020-4706	IBM API Connect 5.0.0.0 through 5.0.8.10 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. By sending a specially HTTP request, a remote attacker could exploit this vulnerability to inject HTTP HOST header, which will allow the attacker to conduct various attacks against the vulner system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 187194.

CVE Number	Description
CVE-2021-39250	Invision Community (aka IPS Community Suite or IP-Board) before 4.6.5.1 allows stored XSS, with resultant code execution, because an uploaded file can be placed ir IFRAME element within user-generated content. For code execution, the attacker can rely on the ability of an admin to install widgets, disclosure of the admin session I Referer header, and the ability of an admin to use the templating engine (e.g., Edit HTML).
CVE-2020-20990	A cross site scripting (XSS) vulnerability in the /segments/edit.php component of Domainmod 4.13 allows attackers to execute arbitrary web scripts or HTML via the Se Name parameter.
CVE-2020-18449	Cross Site Scripting (XSS) vulnerability exists in UKCMS v1.1.10 via data in the index function in Single.php
CVE-2021-36787	The femanager extension before 5.5.1 and 6.x before 6.3.1 for TYPO3 allows XSS via a crafted SVG document.
CVE-2021-36785	The miniorange_saml (aka Miniorange Saml) extension before 1.4.3 for TYPO3 allows XSS.
CVE-2021-38699	TastyIgniter 3.0.7 allows XSS via /account, /reservation, /admin/dashboard, and /admin/system_logs.
CVE-2021-38708	In ocProducts Composr CMS before 10.0.38, an attacker can inject JavaScript via Comcode for XSS.
CVE-2021-32070	The MiCollab Client Service component in Mitel MiCollab before 9.3 could allow an attacker to perform a clickjacking attack due to an insecure header response. A suc exploit could allow an attacker to modify the browser header and redirect users.
CVE-2021-38713	imgURL 2.31 allows XSS via an X-Forwarded-For HTTP header.
CVE-2021-36946	Microsoft Dynamics Business Central Cross-site Scripting Vulnerability
CVE-2021-36950	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability
CVE-2021-27791	The function that is used to parse the Authentication header in Brocade Fabric OS Web application service before Brocade Fabric OS v9.0.1a and v8.2.3a fails to prope process a malformed authentication header from the client, resulting in reading memory addresses outside the intended range. An unauthenticated attacker could disco request, which could bypass the authentication process.
CVE-2021-24471	The YouTube Embed WordPress plugin before 5.2.2 does not validate, escape or sanitise some of its shortcode attributes, leading to Stored XSS issues by 1. using w, controls, cc_lang, color, language, start, stop, or style parameter of youtube shortcode, 2. by using style, class, rel, target, width, height, or alt parameter of youtube_thu shortcode, or 3. by embedding a video whose title or description contains XSS payload (if API key is configured).
CVE-2021-24512	The Video Posts Webcam Recorder WordPress plugin before 3.2.4 has an authenticated reflected cross site scripting (XSS) vulnerability in one of the administrative fu handling deletion of videos.
CVE-2020-20977	A stored cross site scripting (XSS) vulnerability in index.php/legend/6.html of UK CMS v1.1.10 allows attackers to execute arbitrary web scripts or HTML via a crafted p the Comments section.
CVE-2020-21362	A cross site scripting (XSS) vulnerability in the background search function of Maccms10 allows attackers to execute arbitrary web scripts or HTML via the 'wd' parame
CVE-2021-24526	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder WordPress plugin before 1.13.60 does not escape its Form Title before outputting it in attribute when editing a form in the admin dashboard, leading to an authenticated Stored Cross-Site Scripting issue
CVE-2021-24534	The PhoneTrack Meu Site Manager WordPress plugin through 0.1 does not sanitise or escape its "php_id" setting before outputting it back in an attribute in the page, le stored Cross-Site Scripting issue.
CVE-2021-24538	The Current Book WordPress plugin through 1.0.1 does not sanitize user input when an authenticated user adds Author or Book Title, then does not escape these valu outputting to the browser leading to an Authenticated Stored XSS Cross-Site Scripting issue.

CVE Number	Description
CVE-2021-24540	The Wonder Video Embed WordPress plugin before 1.8 does not escape parameters of its wonderplugin_video shortcode, which could allow users with a role as low a Contributor to perform Stored XSS attacks.
CVE-2021-24541	The Wonder PDF Embed WordPress plugin before 1.7 does not escape parameters of its wonderplugin_pdf shortcode, which could allow users with a role as low as C to perform Stored XSS attacks.
CVE-2021-24548	The Mimetic Books WordPress plugin through 0.2.13 was vulnerable to Authenticated Stored Cross-Site Scripting (XSS) in the "Default Publisher ID" field on the plugin page.
CVE-2021-38607	Crocoblock JetEngine before 2.6.1 allows XSS by remote authenticated users via a custom form input.
CVE-2021-38533	NETGEAR RAX40 devices before 1.0.3.64 are affected by stored XSS.
CVE-2021-38752	A cross-site scripting (XSS) vulnerability in Online Catering Reservation System using PHP on Sourcecodester allows an attacker to arbitrarily inject code in the search
CVE-2021-37704	PhpFastCache is a high-performance backend cache system (packagist package phpfastcache/phpfastcache). In versions before 6.1.5, 7.1.2, and 8.0.7 the `phpinfo()` exposed if the `/vendor` is not protected from public access. This is a rare situation today since the vendor directory is often located outside the web directory or protect server rule (.htaccess, etc). Only the v6, v7 and v8 will be patched respectively in 8.0.7, 7.1.2, 6.1.5. Older versions such as v5, v4 are not longer supported and will **N patched. As a workaround, protect the `/vendor` directory from public access.
CVE-2020-20988	A cross site scripting (XSS) vulnerability in the /domains/cost-by-owner.php component of Domainmod 4.13 allows attackers to execute arbitrary web scripts or HTML v crafted payload in the "or Expiring Between" parameter.
CVE-2021-36788	The yoast_seo (aka Yoast SEO) extension before 7.2.3 for TYPO3 allows XSS.
CVE-2021-37693	Discourse is an open-source platform for community discussion. In Discourse before versions 2.7.8 and 2.8.0.beta4, when adding additional email addresses to an exis account on a Discourse site an email token is generated as part of the email verification process. Deleting the additional email address does not invalidate an unused t can then be used in other contexts, including reseting a password.
CVE-2021-38554	HashiCorp Vault and Vault Enterprise's UI erroneously cached and exposed user-viewed secrets between sessions in a single shared browser. Fixed in 1.8.0 and penc 1.6.6 releases.
CVE-2021-37351	Nagios XI before version 5.8.5 is vulnerable to insecure permissions and allows unauthenticated users to access guarded pages through a crafted HTTP request to the
CVE-2021-36791	The dated_news (aka Dated News) extension through 5.1.1 for TYPO3 allows Information Disclosure of application registration data.
CVE-2021-27793	ntermittent authorization failure in aaa tacacs+ with Brocade Fabric OS versions before Brocade Fabric OS v9.0.1b and after 9.0.0, also in Brocade Fabric OS before B Fabric OS v8.2.3a and after v8.2.0 could cause a user with a valid account to be unable to log into the switch.
CVE-2021-22939	If the Node.js https API was used incorrectly and "undefined" was in passed for the "rejectUnauthorized" parameter, no error was returned and connections to servers v expired certificate would have been accepted.
CVE-2021-38755	Unauthenticated doctor entry deletion in Hospital Management System in admin-panel1.php.
CVE-2021-35936	If remote logging is not used, the worker (in the case of CeleryExecutor) or the scheduler (in the case of LocalExecutor) runs a Flask logging server and is listening on a port and also binds on 0.0.0.0 by default. This logging server had no authentication and allows reading log files of DAG jobs. This issue affects Apache Airflow < 2.1.2.
CVE-2021-39241	An issue was discovered in HAProxy 2.0 before 2.0.24, 2.2 before 2.2.16, 2.3 before 2.3.13, and 2.4 before 2.4.3. An HTTP method name may contain a space followe name of a protected resource. It is possible that a server would interpret this as a request for that protected resource, such as in the "GET /admin? HTTP/1.1 /static/ima HTTP/1.1" example.
CVE-2021-37326	NetSarang Xshell 7 before Build 0077 includes unintended code strings in paste operations.

CVE Number	Description
CVE-2021-26086	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to read particular files via a path traversal vulnerability in the /WEB-INF/web.xml endp affected versions are before version 8.5.14, from version 8.6.0 before 8.13.6, and from version 8.14.0 before 8.16.1.
CVE-2021-34485	.NET Core and Visual Studio Information Disclosure Vulnerability
CVE-2021-37586	The PowerPlay Web component of Mitel Interaction Recording Multitenancy systems before 6.7 could allow a user (with Administrator rights) to replay a previously reco conversation of another tenant due to insufficient validation.
CVE-2021-24363	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery WordPress plugin before 1.5.75 did not ensure that uploaded files are kept inside its uploads folder, allov privilege users to put images/SVG anywhere in the filesystem via a path traversal vector
CVE-2021-3045	An OS command argument injection vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator to read any arbitrary file from system. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.19; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PA 9.1.10. PAN-OS 10.0 and later versions are not impacted.
CVE-2020-18455	Cross Site Scripting (XSS) vulnerability exists in bycms v3.0.4 via the title parameter in the edit function in Document.php.
CVE-2020-18456	Cross Site Scripting (XSS) vulnerability exists in PbootCMS v1.3.7 via the title parameter in the mod function in SingleController.php.
CVE-2020-18446	Cross Site Scripting (XSS) vulnerability exists in YUNUCMS 1.1.9 via the param parameter in the insertContent function in ContentModel.php.
CVE-2020-18451	Cross Site Scripting (XSS) vulnerability exists in DamiCMS v6.0.6 via the title parameter in the doadd function in LabelAction.class.php.
CVE-2021-38603	PluXML 5.8.7 allows core/admin/profil.php stored XSS via the Information field.
CVE-2021-35955	Contao >=4.0.0 allows backend XSS via HTML attributes to an HTML field. Fixed in 4.4.56, 4.9.18, 4.11.7.
CVE-2021-38602	PluXML 5.8.7 allows Article Editing stored XSS via Headline or Content.
CVE-2021-24518	The WPFront Notification Bar WordPress plugin before 2.0.0.07176 does not sanitise or escape its Custom CSS setting, allowing high privilege users such as admin to payload in it even when the unfiltered_html capability is disallowed, leading to an authenticated Stored Cross-Site Scripting issue
CVE-2021-29056	Cross Site Scripting (XSS) vulnerability exists in Pixelimity 1.0 via the HTTP POST parameter to admin/setting.php.
CVE-2021-24519	The VikRentCar Car Rental Management System WordPress plugin before 1.1.10 does not sanitise the 'Text Next to Icon' field when adding or editing a Characteristic, high privilege users such as admin to use XSS payload in it, leading to an authenticated Stored Cross-Site Scripting issue
CVE-2021-32069	The AWV component of Mitel MiCollab before 9.3 could allow an attacker to perform a Man-In-the-Middle attack due to improper TLS negotiation. A successful exploit c an attacker to view and modify data.
CVE-2021-1113	NVIDIA camera firmware contains a difficult to exploit vulnerability where a highly privileged attacker can cause unauthorized modification to camera resources, which r in complete denial of service and partial loss of data integrity for all clients.
CVE-2021-38531	Certain NETGEAR devices are affected by incorrect configuration of security settings. This affects D6200 before 1.1.00.40, D7000 before 1.0.1.78, R6020 before 1.0.0. before 1.0.0.42, R6120 before 1.0.0.66, R6260 before 1.1.0.78, R6700v2 before 1.2.0.76, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R7450 before 1.2.0.76, AC before 1.2.0.76, and AC2400 before 1.2.0.76.
CVE-2021-25956	In “Dolibarr” application, v3.3.beta1_20121221 to v13.0.2 have “Modify” access for admin level users to change other user’s details but fails to validate already existing name, while renaming the user “Login”. This leads to complete account takeover of the victim user. This happens since the password gets overwritten for the victim use similar login name.

CVE Number	Description
CVE-2021-31399	On 2N Access Unit 2.0 2.31.0.40.5 devices, an attacker can pose as the web relay for a man-in-the-middle attack.
CVE-2021-32809	ckeditor is an open source WYSIWYG HTML editor with rich content support. A potential vulnerability has been discovered in CKEditor 4 [Clipboard] (https://ckeditor.com/cke4/addon/clipboard) package. The vulnerability allowed to abuse paste functionality using malformed HTML, which could result in injecting arbitr into the editor. It affects all users using the CKEditor 4 plugins listed above at version >= 4.5.2. The problem has been recognized and patched. The fix will be available 4.16.2.
CVE-2021-38524	Certain NETGEAR devices are affected by a stack-based buffer overflow by an authenticated user. This affects MK62 before 1.0.6.110, MR60 before 1.0.6.110, MS60 1.0.6.110, RAX15 before 1.0.2.82, RAX20 before 1.0.2.82, RAX200 before 1.0.3.106, RAX45 before 1.0.2.32, RAX50 before 1.0.2.32, RAX75 before 1.0.3.106, RAX80 1.0.3.106, RBK752 before 3.2.16.6, RBR750 before 3.2.16.6, and RBS750 before 3.2.16.6.
CVE-2021-26428	Azure Sphere Information Disclosure Vulnerability
CVE-2021-1114	NVIDIA Linux kernel distributions contain a vulnerability in the kernel crypto node, where use after free may lead to complete denial of service.
CVE-2021-38553	HashiCorp Vault and Vault Enterprise 1.4.0 through 1.7.3 initialized an underlying database file associated with the Integrated Storage feature with excessively broad fi permissions. Fixed in Vault and Vault Enterprise 1.8.0.
CVE-2021-0083	Improper input validation in some Intel(R) Optane(TM) PMem versions before versions 1.2.0.5446 or 2.2.0.1547 may allow a privileged user to potentially enable denial via local access.
CVE-2021-38586	In cPanel before 98.0.1, /scripts/cpan_config performs unsafe operations on files (SEC-589).
CVE-2021-0008	Uncontrolled resource consumption in firmware for Intel(R) Ethernet Adapters 800 Series Controllers and associated adapters before version 1.5.3.0 may allow privileg potentially enable denial of service via local access.
CVE-2021-0007	Uncaught exception in firmware for Intel(R) Ethernet Adapters 800 Series Controllers and associated adapters before version 1.5.1.0 may allow a privileged attacker to enable denial of service via local access.
CVE-2021-3635	A flaw was found in the Linux kernel netfilter implementation in versions prior to 5.5-rc7. A user with root (CAP_SYS_ADMIN) access is able to panic the system when i netfilter netflow commands.
CVE-2021-0006	Improper conditions check in firmware for Intel(R) Ethernet Adapters 800 Series Controllers and associated adapters before version 1.5.4.0 may allow a privileged user potentially enable denial of service via local access.
CVE-2021-0005	Uncaught exception in firmware for Intel(R) Ethernet Adapters 800 Series Controllers and associated adapters before version 1.5.3.0 may allow a privileged user to pot enable denial of service via local access.
CVE-2021-0004	Improper buffer restrictions in the firmware of Intel(R) Ethernet Adapters 800 Series Controllers and associated adapters before version 1.5.3.0 may allow a privileged u potentially enable denial of service via local access.
CVE-2021-37682	TensorFlow is an end-to-end open source platform for machine learning. In affected versions all TFLite operations that use quantization can be made to use unitialized [For example](https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/lite/kernels/depthwise_conv.cc#L198-L200). Th stems from the fact that `quantization.params` is only valid if `quantization.type` is different that `kTfLiteNoQuantization`. However, these checks are missing in large pa code. We have patched the issue in GitHub commits 537bc7c723439b9194a358f64d871dd326c18887, 4a91f2069f7145aab6ba2d8cfe41be8a110c18a5 and 8933b8a21280696ab119b63263babdb54c298538. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2 TensorFlow 2.3.4, as these are also affected and still in supported range.
CVE-2021-20420	IBM Security Guardium 11.2 could disclose sensitive information due to reliance on untrusted inputs that could aid in further attacks against the system. IBM X-Force ID
CVE-2021-38751	A HTTP Host header attack exists in ExponentCMS 2.6 and below in /exponent_constants.php. A modified HTTP header can change links on the webpage to an arbitra leading to a possible attack vector for MITM.
CVE-2021-21568	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.x contain an insufficient logging vulnerability. An authenticated user with ISI_PRIV_LOGIN_PAPI could make un-aud un-trackable configuration changes to settings that their roles have privileges to change.

CVE Number	Description
CVE-2021-38536	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.40, D7000 before 1.0.1.78, R6020 before 1.0.0.48, R6080 before 1.0.0.48, R6 1.0.0.66, R6260 before 1.1.0.78, R6700v2 before 1.2.0.76, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R6850 before 1.1.0.78, R7200 before 1.2.0.76, R7350 bef 1.2.0.76, R7400 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, AC2600 before 1.2.0.76, RAX35 before 1.0.3.62, and RAX4 1.0.3.62.
CVE-2021-38535	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.40, D7000 before 1.0.1.78, R6020 before 1.0.0.48, R6080 before 1.0.0.48, R6 1.0.0.76, R6260 before 1.1.0.78, R6700v2 before 1.2.0.76, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R6850 before 1.1.0.78, R7200 before 1.2.0.76, R7350 bef 1.2.0.76, R7400 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, AC2600 before 1.2.0.76, RAX35 before 1.0.3.62, and RAX4 1.0.3.62.
CVE-2020-20989	A cross-site request forgery (CSRF) in /admin/maintenance/ of Domainmod 4.13 allows attackers to arbitrarily delete logs.
CVE-2021-38526	Certain NETGEAR devices are affected by a buffer overflow by an unauthenticated attacker. This affects RAX35 before 1.0.3.94, RAX38 before 1.0.3.94, and RAX40 b 1.0.3.94.
CVE-2021-37703	Discourse is an open-source platform for community discussion. In Discourse before versions 2.7.8 and 2.8.0.beta5, a user's read state for a topic such as the last reac number and the notification level is exposed.
CVE-2021-24380	The Shantz WordPress QOTD WordPress plugin through 1.2.2 is lacking any CSRF check when updating its settings, allowing attackers to make logged in administrat them to arbitrary values.
CVE-2021-38537	Certain NETGEAR devices are affected by stored XSS. This affects D6200 before 1.1.00.40, D7000 before 1.0.1.78, R6020 before 1.0.0.48, R6080 before 1.0.0.48, R6 1.0.0.66, R6260 before 1.1.0.78, R6700v2 before 1.2.0.76, R6800 before 1.2.0.76, R6900v2 before 1.2.0.76, R6850 before 1.1.0.78, R7200 before 1.2.0.76, R7350 bef 1.2.0.76, R7400 before 1.2.0.76, R7450 before 1.2.0.76, AC2100 before 1.2.0.76, AC2400 before 1.2.0.76, AC2600 before 1.2.0.76, and RAX40 before 1.0.3.62.
CVE-2021-3047	A cryptographically weak pseudo-random number generator (PRNG) is used during authentication to the Palo Alto Networks PAN-OS web interface. This enables an authenticated attacker, with the capability to observe their own authentication secrets over a long duration on the PAN-OS appliance, to impersonate another authentica interface administrator's session. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.19; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14; PAN-OS 9.1 earlier than PAN-OS 9.1.10; PAN-OS 10.0 versions earlier than PAN-OS 10.0.4. PAN-OS 10.1 versions are not impacted.
CVE-2021-38534	Certain NETGEAR devices are affected by stored XSS. This affects D3600 before 1.0.0.76, D6000 before 1.0.0.76, D6100 before 1.0.0.60, D6200 before 1.1.00.36, D6 1.0.0.52, D6400 before 1.0.0.86, D7000 before 1.0.1.70, D7000v2 before 1.0.0.53, D8500 before 1.0.3.44, DC112A before 1.0.0.42, DGN2200v4 before 1.0.0.110, DGND2200Bv4 before 1.0.0.109, DM200 before 1.0.0.61, JR6150 before 1.0.1.18, PR2000 before 1.0.0.28, R6020 before 1.0.0.42, R6050 before 1.0.1.18, R6080 bef 1.0.0.42, R6220 before 1.1.0.80, R6230 before 1.1.0.80, R6250 before 1.0.4.34, R6260 before 1.1.0.64, R6300v2 before 1.0.4.34, R6400 before 1.0.1.46, R6400v2 bef 1.0.2.62, R6700 before 1.0.2.6, R6700v2 before 1.2.0.36, R6700v3 before 1.0.2.62, R6800 before 1.2.0.36, R6900 before 1.0.2.4, R6900P before 1.3.1.64, R6900v2 b 1.2.0.36, R7000 before 1.0.9.60, R7000P before 1.3.1.64, R7100LG before 1.0.0.50, R7300DST before 1.0.0.70, R7450 before 1.2.0.36, R7900 before 1.0.3.8, R7900 1.4.1.50, R8000 before 1.0.4.28, R8000P before 1.4.1.50, R8300 before 1.0.2.130, R8500 before 1.0.2.130, WNDR3400v3 before 1.0.1.24, WNR2020 before 1.1.0.62, WNR3500Lv2 before 1.2.0.62, XR450 before 2.3.2.40, and XR500 before 2.3.2.40.
CVE-2021-36943	Azure CycleCloud Elevation of Privilege Vulnerability
CVE-2021-32822	The npm hbs package is an Express view engine wrapper for Handlebars. Depending on usage, users of hbs may be vulnerable to a file disclosure vulnerability. There no patch for this vulnerability. hbs mixes pure template data with engine configuration options through the Express render API. By overwriting internal configuration opti disclosure vulnerability may be triggered in downstream applications. For an example PoC see the referenced GHSL-2021-020.
CVE-2021-32830	The @diez/generation npm package is a client for Diez. The locateFont method of @diez/generation has a command injection vulnerability. Clients of the @diez/genera are unlikely to be aware of this, so they might unwittingly write code that contains a vulnerability. This issue may lead to remote code execution if a client of the library c vulnerable method with untrusted input. All versions of this package are vulnerable as of the writing of this CVE.
CVE-2021-32068	The AWV and MiCollab Client Service components in Mitel MiCollab before 9.3 could allow an attacker to perform a Man-In-the-Middle attack by sending multiple sessi renegotiation requests, due to insufficient TLS session controls. A successful exploit could allow an attacker to modify application data and state.
CVE-2020-36473	UCWeb UC 12.12.3.1219 through 12.12.3.1226 uses cleartext HTTP, and thus man-in-the-middle attackers can discover visited URLs.
CVE-2020-18464	Cross Site Request Forgery (CSRF) vulnerability in AikCms 2.0.0 in video_list.php, which can let a malicious user delete movie information.
CVE-2021-33595	A address bar spoofing vulnerability was discovered in Safe Browser for iOS. Showing the legitimate URL in the address bar while loading the content from other doma makes the user believe that the content is served by a legit domain. A remote attacker can leverage this to perform address bar spoofing attack.
CVE-2021-33594	An address bar spoofing vulnerability was discovered in Safe Browser for Android. When user clicks on a specially crafted a malicious URL, it appears like a legitimate address bar, while the content comes from other domain and presented in a window, covering the original content. A remote attacker can leverage this to perform addr spoofing attack.

CVE Number	Description
CVE-2021-38591	An issue was discovered on LG mobile devices with Android OS P and Q software for mt6762/mt6765/mt6883. Attackers can change some of the NvRAM content by le the misconfiguration of a debug command. The LG ID is LVE-SMP-210005 (August 2021).
CVE-2021-21592	Dell EMC PowerScale OneFS versions 8.2.x - 9.2.x improperly handle an exceptional condition. A remote low privileged user could potentially exploit this vulnerability, unauthorized information disclosure.
CVE-2021-32825	bblfshd is an open source self-hosted server for source code parsing. In bblfshd before commit 4265465b9b6fb5663c30ee43806126012066aad4 there is a "zipslip" vul The unsafe handling of symbolic links in an unpacking routine may enable attackers to read and/or write to arbitrary locations outside the designated target folder. This lead to arbitrary file write (with same permissions as the program running the unpack operation) if the attacker can control the archive file. Additionally, if the attacker ha access to the unpacked files, he may be able to read arbitrary system files the parent process has permissions to read. For more details including a PoC see the refere GHSL-2020-258.
CVE-2021-36282	Dell EMC PowerScale OneFS versions 8.2.x - 9.1.0.x contain a use of uninitialized resource vulnerability. This can potentially allow an authenticated user with ISI_PRIV_LOGIN_CONSOLE or ISI_PRIV_LOGIN_SSH privileges to gain access up to 24 bytes of data within the /ifs kernel stack under certain conditions.
CVE-2020-18463	Cross Site Request Forgery (CSRF) vulnerability exists in v2.0.0 in video_list.php, which can let a malicious user delete a video message.
CVE-2021-38514	Certain NETGEAR devices are affected by authentication bypass. This affects D3600 before 1.0.0.72, D6000 before 1.0.0.72, D6100 before 1.0.0.63, D6200 before 1.1 D6220 before 1.0.0.48, D6400 before 1.0.0.86, D7000 before 1.0.1.70, D7000v2 before 1.0.0.52, D7800 before 1.0.1.56, D8500 before 1.0.3.44, DC112A before 1.0.0. DGN2200v4 before 1.0.0.108, DGND2200Bv4 before 1.0.0.108, EX2700 before 1.0.1.48, EX3700 before 1.0.0.76, EX3800 before 1.0.0.76, EX6000 before 1.0.0.38, E before 1.0.2.24, EX6100v2 before 1.0.1.76, EX6120 before 1.0.0.42, EX6130 before 1.0.0.28, EX6150v1 before 1.0.0.42, EX6150v2 before 1.0.1.76, EX6200 before 1. EX6200v2 before 1.0.1.72, EX6400 before 1.0.2.136, EX7000 before 1.0.0.66, EX7300 before 1.0.2.136, EX8000 before 1.0.1.180, RBK50 before 2.1.4.10, RBR50 bef 2.1.4.10, RBS50 before 2.1.4.10, RBK40 before 2.1.4.10, RBR40 before 2.1.4.10, RBS40 before 2.1.4.10, RBW30 before 2.2.1.204, PR2000 before 1.0.0.28, R6020 b 1.0.0.38, R6080 before 1.0.0.38, R6050 before 1.0.1.18, JR6150 before 1.0.1.18, R6120 before 1.0.0.46, R6220 before 1.1.0.86, R6250 before 1.0.4.34, R6300v2 befo 1.0.4.32, R6400 before 1.0.1.44, R6400v2 before 1.0.2.62, R6700 before 1.0.1.48, R6700v2 before 1.2.0.36, R6800 before 1.2.0.36, R6900v2 before 1.2.0.36, R6900 I 1.0.1.48, R7000 before 1.0.9.34, R6900P before 1.3.1.64, R7000P before 1.3.1.64, R7100LG before 1.0.0.48, R7300DST before 1.0.0.70, R7500v2 before 1.0.3.38, R7 before 1.0.2.52, R7900 before 1.0.3.8, R8000 before 1.0.4.28, R7900P before 1.4.1.30, R8000P before 1.4.1.30, R8300 before 1.0.2.128, R8500 before 1.0.2.128, R9(1.0.3.10, RBS40V before 2.2.0.58, RBK50V before 2.2.0.58, WN2000RPTv3 before 1.0.1.32, WN2500RPv2 before 1.0.1.54, WN3000RPv3 before 1.0.2.78, WN3100R 1.0.0.66, WNDR3400v3 before 1.0.1.22, WNDR3700v4 before 1.0.2.102, WNDR4300v1 before 1.0.2.104, WNDR4300v2 before 1.0.0.56, WNDR4500v3 before 1.0.0.5 WNR2000v5 (R2000) before 1.0.0.66, WNR2020 before 1.1.0.62, WNR2050 before 1.1.0.62, WNR3500Lv2 before 1.2.0.62, and XR500 before 2.3.2.22.
CVE-2021-33791	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability
CVE-2021-34407	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-30480. Reason: This candidate is a reservation duplicate of CVE-2021-30480. N CVE users should reference CVE-2021-30480 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usa
CVE-2020-21064	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2019-15048. Reason: This candidate is a reservation duplicate of CVE-2019-15048. N CVE users should reference CVE-2019-15048 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usa