SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 19 May 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	Reference
CVE-2021-28799	An improper authorization vulnerability has been reported to affect QNAP NAS running HBS 3 (Hybrid Backup Sync.) If exploited, the vulnerability allows remote attackers to log in to a device. This issue affects: QNAP Systems Inc. HBS 3 versions prior to v16.0.0415 on QTS 4.5.2; versions prior to v3.0.210412 on QTS 4.3.6; versions prior to v3.0.210411 on QTS 4.3.4; versions prior to v3.0.210411 on QTS 4.3.3; versions prior to v16.0.0419 on QuTS hero h4.5.1; versions prior to v16.0.0419 on QuTScloud c4.5.1~c4.5.4. This issue does not affect: QNAP Systems Inc. HBS 2 . QNAP Systems Inc. HBS 1.3 .	10.0	More Details
CVE-2021-20998	In multiple managed switches by WAGO in different versions without authorization and with specially crafted packets it is possible to create users.	10.0	More Details
CVE-2020-35198	An issue was discovered in Wind River VxWorks 7. The memory allocator has a possible integer overflow in calculating a memory block's size to be allocated by calloc(). As a result, the actual memory allocated is smaller than the buffer size specified by the arguments, leading to memory corruption.	9.8	More Details
CVE-2020-13873	A SQL Injection vulnerability in get_topic_info() in sys/CODOF/Forum/Topic.php in Codoforum before 4.9 allows remote attackers (pre-authentication) to bypass the admin page via a leaked password-reset token of the admin. (As an admin, an attacker can upload a PHP shell and execute remote code on the operating system.)	9.8	More Details
CVE-2021-31316	The unprivileged user portal part of CentOS Web Panel is affected by a SQL Injection via the 'idsession' HTTP POST parameter.	9.8	More Details
CVE-2020-18178	Path Traversal in HongCMS v4.0.0 allows remote attackers to view, edit, and delete arbitrary files via a crafted POST request to the component "/hcms/admin/index.php/language/ajax."	9.8	More Details
CVE-2021-32305	WebSVN before 2.6.1 allows remote attackers to execute arbitrary commands via shell metacharacters in the search parameter.	9.8	More Details
CVE-2020-20951	In Pluck-4.7.10-dev2 admin background, a remote command execution vulnerability exists when uploading files.	9.8	More Details
CVE-2021-24314	The Goto WordPress theme before 2.1 did not sanitise, validate of escape the keywords GET parameter from its listing page before using it in a SQL statement, leading to an Unauthenticated SQL injection issue	9.8	More Details
CVE-2021-27734	Hirschmann HiOS 07.1.01, 07.1.02, and 08.1.00 through 08.5.xx and HiSecOS 03.3.00 through 03.5.01 allow remote attackers to change the credentials of existing users.	9.8	More Details
CVE-2021-22668	Delta Industrial Automation CNCSoft ScreenEditor Versions 1.01.28 (with ScreenEditor Version 1.01.2) and prior are vulnerable to an out-of-bounds read while processing project files, which may allow an attacker to execute arbitrary code.	9.8	More Details
CVE-2020-23691	YFCMF v2.3.1 has a Remote Command Execution (RCE) vulnerability in the index.php.	9.8	More Details
CVE-2021-25943	Prototype pollution vulnerability in '101' versions 1.0.0 through 1.6.3 allows an attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2021-25941	Prototype pollution vulnerability in 'deep-override' versions 1.0.0 through 1.0.1 allows an attacker to cause a denial of service and may lead to remote code execution.	9.8	More Details
CVE-2020-18166	Unrestricted File Upload in LAOBANCMS v2.0 allows remote attackers to upload arbitrary files by attaching a file with a ".jpg.php" extension to the component "admin/wenjian.php?wj=../templets/pc".	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24285	The request_list_request AJAX call of the Car Seller - Auto Classifieds Script WordPress plugin through 2.1.0, available to both authenticated and unauthenticated users, does not sanitise, validate or escape the order_id POST parameter before using it in a SQL statement, leading to a SQL Injection issue.	9.8	More Details
CVE-2021-24284	The Kaswara Modern VC Addons WordPress plugin through 3.0.1 allows unauthenticated arbitrary file upload via the 'uploadFontIcon' AJAX action. The supplied zipfile being unzipped in the wp-content/uploads/kaswara/fonts_icon directory with no checks for malicious files such as PHP.	9.8	More Details
CVE-2021-33026	The Flask-Caching extension through 1.10.1 for Flask relies on Pickle for serialization, which may lead to remote code execution or local privilege escalation. If an attacker gains access to cache storage (e.g., filesystem, Memcached, Redis, etc.), they can construct a crafted payload, poison the cache, and execute Python code. NOTE: a third party indicates that exploitation is extremely unlikely unless the machine is already compromised; in other cases, the attacker would be unable to write their payload to the cache and generate the required collision	9.8	More Details
CVE-2021-32615	Piwigo 11.4.0 allows admin/user_list_backend.php order[0][dir] SQL Injection.	9.8	More Details
CVE-2020-28063	A file upload issue exists in all versions of ArticleCMS which allows malicious users to getshell.	9.8	More Details
CVE-2020-20092	File Upload vulnerability exists in ArticleCMS 1.0 via the image upload feature at /admin by changing the Content-Type to image/jpeg and placing PHP code after the JPEG data, which could let a remote malicious user execute arbitrary PHP code.	9.8	More Details
CVE-2020-23790	An Arbitrary File Upload vulnerability was discovered in the Golo Laravel theme v 1.1.5.	9.8	More Details
CVE-2021-32608	An issue was discovered in Smartstore (aka SmartStoreNET) through 4.1.1. Views/Boards/Partials/_ForumPost.cshtml does not call HtmlUtils.SanitizeHtml on certain text for a forum post.	9.8	More Details
CVE-2021-32607	An issue was discovered in Smartstore (aka SmartStoreNET) through 4.1.1. Views/PrivateMessages/View.cshtml does not call HtmlUtils.SanitizeHtml on a private message.	9.8	More Details
CVE-2021-27384	A vulnerability has been identified in SIMATIC HMI Comfort Outdoor Panels V15 7\" & 15\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SIMATIC HMI Comfort Outdoor Panels V16 7\" & 15\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI Comfort Panels V15 4\" - 22\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SIMATIC HMI Comfort Panels V16 4\" - 22\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI KTP Mobile Panels V15 KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V15.1 Update 6), SIMATIC HMI KTP Mobile Panels V16 KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V16 Update 4), SIMATIC WinCC Runtime Advanced V15 (All versions < V15.1 Update 6), SIMATIC WinCC Runtime Advanced V16 (All versions < V16 Update 4), SINAMICS GH150 (All versions), SINAMICS GL150 (with option X30) (All versions), SINAMICS GM150 (with option X30) (All versions), SINAMICS SH150 (All versions), SINAMICS SL150 (All versions), SINAMICS SM120 (All versions), SINAMICS SM150 (All versions), SINAMICS SM150i (All versions). SmartVNC has an out-of-bounds memory access vulnerability in the device layout handler, represented by a binary data stream on client side, which can potentially result in code execution.	9.8	More Details
CVE-2021-31324	The unprivileged user portal part of CentOS Web Panel is affected by a Command Injection vulnerability leading to root Remote Code Execution.	9.8	More Details
CVE-2021-32454	SITEL CAP/PRX firmware version 5.2.01 makes use of a hardcoded password. An attacker with access to the device could modify these credentials, leaving the administrators of the device without access.	9.6	More Details
CVE-2021-20999	In Weidmüller u-controls and IoT-Gateways in versions up to 1.12.1 a network port intended only for device-internal usage is accidentally accessible via external network interfaces. By exploiting this vulnerability the device may be manipulated or the operation may be stopped.	9.4	More Details
CVE-2021-3402	An integer overflow and several buffer overflow reads in libyara/modules/macho/macho.c in YARA v4.0.3 and earlier could allow an attacker to either cause denial of service or information disclosure via a malicious Mach-O file. Affects all versions before libyara 4.0.4	9.1	More Details
CVE-2020-4669	IBM Planning Analytics Local 2.0 connects to a MongoDB server. MongoDB, a document-oriented database system, is listening on the remote port, and it is configured to allow connections without password authentication. A remote attacker can gain unauthorized access to the database. IBM X-Force ID: 184600.	9.1	More Details
CVE-2020-4670	IBM Planning Analytics Local 2.0 connects to a Redis server. The Redis server, an in-memory data structure store, running on the remote host is not protected by password authentication. A remote attacker can exploit this to gain unauthorized access to the server. IBM X-Force ID: 186401.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2021-3518	There's a flaw in libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by an application linked with libxml2 could trigger a u greatest impact from this flaw is to confidentiality, integrity, and availability.

CVE Number	Description
CVE-2020-21830	A heap based buffer overflow vulneraibility exists in GNU LibreDWG 0.10 via bit_calc_CRC ../../src/bits.c:2213.
CVE-2020-21841	A heap based buffer overflow vulnerability exits in GNU LibreDWG 0.10 via bit_read_B ../../src/bits.c:135.
CVE-2021-22866	A UI misrepresentation vulnerability was identified in GitHub Enterprise Server that allowed more permissions to be granted during a GitHub App's user-authorization w displayed to the user during approval. To exploit this vulnerability, an attacker would need to create a GitHub App on the instance and have a user authorize the applica authentication flow. All permissions being granted would properly be shown during the first authorization, but in certain circumstances, if the user revisits the authorizati App has configured additional user-level permissions, those additional permissions may not be shown, leading to more permissions being granted than the user potenti vulnerability affected GitHub Enterprise Server 3.0.x prior to 3.0.7 and 2.22.x prior to 2.22.13. It was fixed in versions 3.0.7 and 2.22.13. This vulnerability was reported Bounty program.
CVE-2020-21840	A heap based buffer overflow vulnerability exits in GNU LibreDWG 0.10 via bit_search_sentinel ../../src/bits.c:1985.
CVE-2020-21838	A heap based buffer overflow vulnerability exits in GNU LibreDWG 0.10 via: read_2004_section_appinfo ../../src/decode.c:2842.
CVE-2020-21836	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_section_preview ../../src/decode.c:3175.
CVE-2021-32073	DedeCMS V5.7 SP2 contains a CSRF vulnerability that allows a remote attacker to send a malicious request to to the web manager allowing remote code execution.
CVE-2020-21833	A heap based buffer overflow vulnerability exits in GNU LibreDWG 0.10 via: read_2004_section_classes ../../src/decode.c:2440.
CVE-2021-29053	Multiple SQL injection vulnerabilities in Liferay Portal 7.3.5 and Liferay DXP 7.3 before fix pack 1 allow remote authenticated users to execute arbitrary SQL commands parameter to (1) CommerceChannelRelFinder.countByC_C, or (2) CommerceChannelRelFinder.findByC_C.
CVE-2020-21832	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_compressed_section ../../src/decode.c:2417.
CVE-2021-22155	An Authentication Bypass vulnerability in the SAML Authentication component of BlackBerry Workspaces Server (deployed with Appliance-X) version(s) 10.1, 9.1 and e attacker to potentially gain access to the application in the context of the targeted user's account.
CVE-2020-21831	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_section_handles ../../src/decode.c:2637.
CVE-2021-3528	A flaw was found in noobaa-operator in versions before 5.7.0, where internal RPC AuthTokens between the noobaa operator and the noobaa core are leaked into log fi access to the log files could use this AuthToken to gain additional access into noobaa deployment and can read/modify system configuration.
CVE-2021-31215	SchedMD Slurm before 20.02.7 and 20.03.x through 20.11.x before 20.11.7 allows remote code execution as SlurmUser because use of a PrologSlurmctld or EpilogSl environment mishandling.
CVE-2021-32402	Intelbras Router RF 301K Firmware 1.1.2 is vulnerable to Cross Site Request Forgery (CSRF) due to lack of validation and insecure configurations in inputs and modul
CVE-2021-32403	Intelbras Router RF 301K Firmware 1.1.2 is vulnerable to Cross Site Request Forgery (CSRF) due to lack of security mechanisms for token protection and unsafe input
CVE-2020-21819	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10.2641via htmlescape ../../programs/escape.c:51.
CVE-2020-21818	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10.2641 via htmlescape ../../programs/escape.c:48.

CVE Number	Description
CVE-2020-21816	A heab based buffer overflow issue exists in GNU LibreDWG 0.10.2641 via htmlescape ../../programs/escape.c:46.
CVE-2021-24289	There is functionality in the Store Locator Plus for WordPress plugin through 5.5.14 that made it possible for authenticated users to update their user meta data to beco any site using the plugin.
CVE-2021-20994	In multiple managed switches by WAGO in different versions an attacker may trick a legitimate user to click a link to inject possible malicious code into the Web-Based
CVE-2020-18198	Cross Site Request Forgery (CSRF) in Pluck CMS v4.7.9 allows remote attackers to execute arbitrary code and delete specific images via the component " /admin.php
CVE-2020-18195	Cross Site Request Forgery (CSRF) in Pluck CMS v4.7.9 allows remote attackers to execute arbitrary code and delete a specific article via the component " /admin.php
CVE-2020-21842	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_section_revhistory ../../src/decode.c:3051.
CVE-2021-24188	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the WP Content Copy Protection & No Right Click WordPress plugin before plugin (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins a critical vulnerabilities like RCE.
CVE-2021-31827	In Progress MOVEit Transfer before 2021.0 (13.0), a SQL injection vulnerability has been found in the MOVEit Transfer web app that could allow an authenticated attac unauthorized access to MOVEit Transfer's database. Depending on the database engine being used (MySQL, Microsoft SQL Server, or Azure SQL), an attacker may b information about the structure and contents of the database in addition to executing SQL statements that alter or destroy database elements. This is in MOVEit.DMZ.W SILHuman.vb.
CVE-2021-24280	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, any authenticated user, such as a subscriber, could use the import_from_debug AJAX action to ir
CVE-2021-24195	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the Login as User or Customer (User Switching) WordPress plugin before 1 (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins and cou vulnerabilities like RCE.
CVE-2021-24194	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the Login Protection - Limit Failed Login Attempts WordPress plugin before plugin (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins a critical vulnerabilities like RCE.
CVE-2021-24193	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the Visitor Traffic Real Time Statistics WordPress plugin before 2.12, to inst (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins and cou vulnerabilities like RCE.
CVE-2021-24192	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the Tree Sitemap WordPress plugin before 2.9, to install any plugin (includi from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins and could lead to more critical vulnera
CVE-2021-24191	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the WP Maintenance Mode & Site Under Construction WordPress plugin be any plugin (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugi more critical vulnerabilities like RCE.
CVE-2021-24190	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the WooCommerce Conditional Marketing Mailer WordPress plugin before plugin (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins a critical vulnerabilities like RCE.
CVE-2021-24189	Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the Captchinoo, Google recaptcha for admin login page WordPress plugin b plugin (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins a critical vulnerabilities like RCE.
CVE-2020-23996	A local file inclusion vulnerability in ILIAS before 5.3.19, 5.4.10 and 6.0 allows remote authenticated attackers to execute arbitrary code via the import of personal data.
CVE-2020-21844	GNU LibreDWG 0.10 is affected by: memcpy-param-overlap. The impact is: execute arbitrary code (remote). The component is: read_2004_section_header ../../src/dec
CVE-2020-21843	A heap based buffer overflow vulnerability exits in GNU LibreDWG 0.10 via bit_read_RC ../../src/bits.c:318.

CVE Number	Description
CVE-2020-21814	A heap based buffer overflow issue exists in GNU LibreDWG 0.10.2641 via htmlwescape ../../programs/escape.c:97.
CVE-2021-20988	In Hilscher rcX RTOS versions prios to V2.1.14.1 the actual UDP packet length is not verified against the length indicated by the packet. This may lead to a denial of se device.
CVE-2021-32820	Express-handlebars is a Handlebars view engine for Express. Express-handlebars mixes pure template data with engine configuration options through the Express ren specifically, the layout parameter may trigger file disclosure vulnerabilities in downstream applications. This potential vulnerability is somewhat restricted in that only file extentions (i.e. file.extension) can be included, files that lack an extension will have .handlebars appended to them. For complete details refer to the referenced GHSL-2 in documentation have been added to help users avoid this potential information exposure vulnerability.
CVE-2021-23892	By exploiting a time of check to time of use (TOCTOU) race condition during the Endpoint Security for Linux Threat Prevention and Firewall (ENSL TP/FW) installation can perform a privilege escalation attack to obtain administrator privileges for the purpose of executing arbitrary code through insecure use of predictable temporary file
CVE-2021-32819	Squirrelly is a template engine implemented in JavaScript that works out of the box with ExpressJS. Squirrelly mixes pure template data with engine configuration optio render API. By overwriting internal configuration options remote code execution may be triggered in downstream applications. This issue is fixed in version 9.0.0. For co the referenced GHSL-2021-023.
CVE-2021-3423	Uncontrolled Search Path Element vulnerability in the openssl component as used in Bitdefender GravityZone Business Security allows an attacker to load a third party privileges. This issue affects Bitdefender GravityZone Business Security versions prior to 6.6.23.329.
CVE-2020-21827	A heap based buffer overflow vulnerability exists in GNU LibreDWG 0.10 via read_2004_compressed_section ../../src/decode.c:2379.
CVE-2020-24755	In Ubiquiti UniFi Video v3.10.13, when the executable starts, its first library validation is in the current directory. This allows the impersonation and modification of the lib on the system. This was tested in (Windows 7 x64/Windows 10 x64).
CVE-2021-27413	Omron CX-One Versions 4.60 and prior, including CX-Server Versions 5.0.29.0 and prior, are vulnerable to a stack-based buffer overflow, which may allow an attacker code.
CVE-2021-20025	SonicWall Email Security Virtual Appliance version 10.0.9 and earlier versions contain a default username and a password that is used at initial setup. An attacker coul transitional/temporary user account from the trusted domain to access the Virtual Appliance remotely only when the device is freshly installed and not connected to Mys
CVE-2020-27823	A flaw was found in OpenJPEG's encoder. This flaw allows an attacker to pass specially crafted x,y offset input to OpenJPEG to use during encoding. The highest threa is to confidentiality, integrity, as well as system availability.
CVE-2021-32238	Epic Games / Psyonix Rocket League <=1.95 is affected by Buffer Overflow. Stack-based buffer overflow occurs when Rocket League handles UPK object files that ca execution and denial of service scenario.
CVE-2021-30145	A format string vulnerability in mpv through 0.33.0 allows user-assisted remote attackers to achieve code execution via a crafted m3u playlist file.
CVE-2021-22117	RabbitMQ installers on Windows prior to version 3.8.16 do not harden plugin directory permissions, potentially allowing attackers with sufficient local filesystem permiss plugins.
CVE-2020-21813	A heap based buffer overflow issue exists in GNU LibreDWG 0.10.2641 via output_TEXT ../../programs/dwg2SVG.c:114.
CVE-2021-31728	Incorrect access control in zam64.sys, zam32.sys in MalwareFox AntiMalware 2.74.0.150 allows a non-privileged process to open a handle to \.\ZemanaAntiMalware, r driver by sending IOCTL 0x80002010, allocate executable memory using a flaw in IOCTL 0x80002040, install a hook with IOCTL 0x80002044 and execute the executa hook with IOCTL 0x80002014 or 0x80002018, this exposes ring 0 code execution in the context of the driver allowing the non-privileged process to elevate privileges.
CVE-2021-27397	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V16.0.5). The PlantSimCore.dll library lacks proper validation of user-supplied data wh This could result in a memory corruption condition. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-13287)
CVE-2021-27396	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V16.0.5). The PlantSimCore.dll library lacks proper validation of user-supplied data wh This could result in a stack based buffer overflow, a different vulnerability than CVE-2021-27398. An attacker could leverage this vulnerability to execute code in the co process. (ZDI-CAN-13279)
CVE-2019-25044	The block subsystem in the Linux kernel before 5.2 has a use-after-free that can lead to arbitrary code execution in the kernel context and privilege escalation, aka CID related to blk_mq_free_rqs and blk_cleanup_queue.

CVE Number	Description
CVE-2021-33033	The Linux kernel before 5.11.14 has a use-after-free in cipso_v4_genopt in net/ipv4/cipso_ipv4.c because the CIPSO and CALIPSO refcounting for the DOI definitions CID-ad5d07f4a9cd. This leads to writing an arbitrary value.
CVE-2021-33034	In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary
CVE-2021-23134	Use After Free vulnerability in nfc sockets in the Linux Kernel before 5.12.4 allows local attackers to elevate their privileges. In typical configurations, the issue can only privileged local user with the CAP_NET_RAW capability.
CVE-2021-3483	A flaw was found in the Nosy driver in the Linux kernel. This issue allows a device to be inserted twice into a doubly-linked list, leading to a use-after-free when one of t removed. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. Versions before kernel 5.12-rc6 are affected
CVE-2021-31727	Incorrect access control in zam64.sys, zam32.sys in MalwareFox AntiMalware 2.74.0.150 where IOCTL's 0x80002014, 0x80002018 expose unrestricted disk read/write respectively. A non-privileged process can open a handle to \.\ZemanaAntiMalware, register with the driver using IOCTL 0x80002010 and send these IOCTL's to escala overwriting the boot sector or overwriting critical code in the pagefile.
CVE-2021-27398	A vulnerability has been identified in Tecnomatix Plant Simulation (All versions < V16.0.5). The PlantSimCore.dll library lacks proper validation of user-supplied data wh This could result in a stack based buffer overflow, a different vulnerability than CVE-2021-27396. An attacker could leverage this vulnerability to execute code in the cor process. (ZDI-CAN-13290)
CVE-2021-23891	Privilege Escalation vulnerability in McAfee Total Protection (MTP) prior to 16.0.32 allows a local user to gain elevated privileges by impersonating a client token which bypassing of MTP self-defense.
CVE-2021-23872	Privilege Escalation vulnerability in the File Lock component of McAfee Total Protection (MTP) prior to 16.0.32 allows a local user to gain elevated privileges by manipu the IOCTL interface.
CVE-2021-25694	Teradici PCoIP Graphics Agent for Windows prior to 21.03 does not validate NVENC.dll. An attacker could replace the .dll and redirect pixels elsewhere.
CVE-2021-32818	haml-coffee is a JavaScript templating solution. haml-coffee mixes pure template data with engine configuration options through the Express render API. More specifica supports overriding a series of HTML helper functions through its configuration options. A vulnerable application that passes user controlled request objects to the haml may introduce RCE vulnerabilities. Additionally control over the escapeHtml parameter through template configuration pollution ensures that haml-coffee would not san that may result in reflected Cross Site Scripting attacks against downstream applications. There is currently no fix for these issues as of the publication of this CVE. The coffee is currently 1.14.1. For complete details refer to the referenced GHSL-2021-025.
CVE-2021-25660	A vulnerability has been identified in SIMATIC HMI Comfort Outdoor Panels V15 7\" & 15\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SIMATIC HMI Comf 7\" & 15\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI Comfort Panels V15 4\" - 22\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SI Panels V16 4\" - 22\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI KTP Mobile Panels V15 KTP400F, KTP700, KTP700F, KTP900 and KTP900 Update 6), SIMATIC HMI KTP Mobile Panels V16 KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V16 Update 4), SIMATIC WinCC Runtime Adva < V15.1 Update 6), SIMATIC WinCC Runtime Advanced V16 (All versions < V16 Update 4). SmartVNC has an out-of-bounds memory access vulnerability that could b server side when sending data from the client, which could result in a Denial-of-Service condition.
CVE-2021-20393	IBM QRadar User Behavior Analytics 1.0.0 through 4.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returr information could be used in further attacks against the system. IBM X-Force ID: 196001.
CVE-2021-27386	A vulnerability has been identified in SIMATIC HMI Comfort Outdoor Panels V15 7\" & 15\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SIMATIC HMI Comf 7\" & 15\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI Comfort Panels V15 4\" - 22\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SI Panels V16 4\" - 22\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI KTP Mobile Panels V15 KTP400F, KTP700, KTP700F, KTP900 and KTP900 Update 6), SIMATIC HMI KTP Mobile Panels V16 KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V16 Update 4), SIMATIC WinCC Runtime Adva < V15.1 Update 6), SIMATIC WinCC Runtime Advanced V16 (All versions < V16 Update 4), SINAMICS GH150 (All versions), SINAMICS GL150 (with option X30) (All GM150 (with option X30) (All versions), SINAMICS SH150 (All versions), SINAMICS SL150 (All versions), SINAMICS SM120 (All versions), SINAMICS SM150 (All vers SM150i (All versions). SmartVNC has a heap allocation leak vulnerability in the device layout handler on client side, which could result in a Denial-of-Service condition.
CVE-2002-2438	TCP firewalls could be circumvented by sending a SYN Packets with other flags (like e.g. RST flag) set, which was not correctly discarded by the Linux TCP stack after
CVE-2021-31922	An HTTP Request Smuggling vulnerability in Pulse Secure Virtual Traffic Manager before 21.1 could allow an attacker to smuggle an HTTP request through an HTTP/2 vulnerability is resolved in 21.1, 20.3R1, 20.2R1, 20.1R2, 19.2R4, and 18.2R3.
CVE-2021-32051	Hexagon G!nius Auskunftsportal before 5.0.0.0 allows SQL injection via the GiPWorkflow/Service/DownloadPublicFile id parameter.
CVE-2020-27020	Password generator feature in Kaspersky Password Manager was not completely cryptographically strong and potentially allowed an attacker to predict generated pass An attacker would need to know some additional information (for example, time of password generation).

CVE Number	Description
CVE-2021-30183	Cleartext storage of sensitive information in multiple versions of Octopus Server where in certain situations when running import or export processes, the password use decrypt sensitive values would be written to the logs in plaintext.
CVE-2021-24278	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, unauthenticated users can use the wpcf7r_get_nonce AJAX action to retrieve a valid nonce for ar action/function.
CVE-2020-4985	IBM Planning Analytics Local 2.0 could allow an attacker to obtain sensitive information due to accepting body parameters in a query. IBM X-Force ID: 192642.
CVE-2021-20277	A flaw was found in Samba's libldb. Multiple, consecutive leading spaces in an LDAP attribute can lead to an out-of-bounds memory write, leading to a crash of the LDA handling the request. The highest threat from this vulnerability is to system availability.
CVE-2020-25709	A flaw was found in OpenLDAP. This flaw allows an attacker who can send a malicious packet to be processed by OpenLDAP's slapd server, to trigger an assertion fai from this vulnerability is to system availability.
CVE-2020-27150	In multiple versions of NPort IA5000A Series, the result of exporting a device's configuration contains the passwords of all users on the system and other sensitive data "Pre-shared key" doesn't set.
CVE-2021-27385	A vulnerability has been identified in SIMATIC HMI Comfort Outdoor Panels V15 7\" & 15\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SIMATIC HMI Comf 7\" & 15\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI Comfort Panels V15 4\" - 22\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SI Panels V16 4\" - 22\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI KTP Mobile Panels V15 KTP400F, KTP700, KTP700F, KTP900 and KTP900 Update 6), SIMATIC HMI KTP Mobile Panels V16 KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V16 Update 4), SIMATIC WinCC Runtime Adva < V15.1 Update 6), SIMATIC WinCC Runtime Advanced V16 (All versions < V16 Update 4), SINAMICS GH150 (All versions), SINAMICS GL150 (with option X30) (All GM150 (with option X30) (All versions), SINAMICS SH150 (All versions), SINAMICS SL150 (All versions), SINAMICS SM120 (All versions), SINAMICS SM150 (All vers SM150i (All versions). A remote attacker could send specially crafted packets to SmartVNC device layout handler on client side, which could influence the amount of re result in a Denial-of-Service (infinite loop) condition.
CVE-2021-27383	A vulnerability has been identified in SIMATIC HMI Comfort Outdoor Panels V15 7\" & 15\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SIMATIC HMI Comf 7\" & 15\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI Comfort Panels V15 4\" - 22\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SI Panels V16 4\" - 22\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI KTP Mobile Panels V15 KTP400F, KTP700, KTP700F, KTP900 and KTP900 Update 6), SIMATIC HMI KTP Mobile Panels V16 KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V16 Update 4), SIMATIC WinCC Runtime Adva < V15.1 Update 6), SIMATIC WinCC Runtime Advanced V16 (All versions < V16 Update 4), SINAMICS GH150 (All versions), SINAMICS GL150 (with option X30) (All GM150 (with option X30) (All versions), SINAMICS SH150 (All versions), SINAMICS SL150 (All versions), SINAMICS SM120 (All versions), SINAMICS SM150 (All vers SM150i (All versions). SmartVNC has a heap allocation leak vulnerability in the server Tight encoder, which could result in a Denial-of-Service condition.
CVE-2020-25242	A vulnerability has been identified in SIMATIC NET CP 343-1 Advanced (incl. SIPLUS variants) (All versions), SIMATIC NET CP 343-1 Lean (incl. SIPLUS variants) (Al NET CP 343-1 Standard (incl. SIPLUS variants) (All versions). Specially crafted packets sent to TCP port 102 could cause a Denial-of-Service condition on the affected might be necessary in order to recover.
CVE-2020-28393	An unauthenticated remote attacker could create a permanent denial-of-service condition by sending specially crafted OSPF packets. Successful exploitation requires (an affected device on the SCALANCE XM-400, XR-500 (All versions prior to v6.4).
CVE-2021-25661	A vulnerability has been identified in SIMATIC HMI Comfort Outdoor Panels V15 7\" & 15\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SIMATIC HMI Comf 7\" & 15\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI Comfort Panels V15 4\" - 22\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SI Panels V16 4\" - 22\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI KTP Mobile Panels V15 KTP400F, KTP700, KTP700F, KTP900 and KTP900 Update 6), SIMATIC HMI KTP Mobile Panels V16 KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V16 Update 4), SIMATIC WinCC Runtime Adva < V15.1 Update 6), SIMATIC WinCC Runtime Advanced V16 (All versions < V16 Update 4). SmartVNC has an out-of-bounds memory access vulnerability that could b side when sending data from the server, which could result in a Denial-of-Service condition.
CVE-2021-25662	A vulnerability has been identified in SIMATIC HMI Comfort Outdoor Panels V15 7\" & 15\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SIMATIC HMI Comf 7\" & 15\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI Comfort Panels V15 4\" - 22\" (incl. SIPLUS variants) (All versions < V15.1 Update 6), SI Panels V16 4\" - 22\" (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI KTP Mobile Panels V15 KTP400F, KTP700, KTP700F, KTP900 and KTP900 Update 6), SIMATIC HMI KTP Mobile Panels V16 KTP400F, KTP700, KTP700F, KTP900 and KTP900F (All versions < V16 Update 4), SIMATIC WinCC Runtime Adva < V15.1 Update 6), SIMATIC WinCC Runtime Advanced V16 (All versions < V16 Update 4). SmartVNC client fails to handle an exception properly if the program execu modified after sending a packet from the server, which could result in a Denial-of-Service condition.
CVE-2021-20997	In multiple managed switches by WAGO in different versions it is possible to read out the password hashes of all Web-based Management users.
CVE-2021-32919	An issue was discovered in Prosody before 0.11.9. The undocumented dialback_without_dialback option in mod_dialback enables an experimental feature for server-to It does not correctly authenticate remote server certificates, allowing a remote server to impersonate another server (when this option is enabled).
CVE-2021-32611	A NULL pointer dereference vulnerability exists in eXcall_api.c in Antisip eXosip2 through 5.2.0 when handling certain 3xx redirect responses.

CVE Number	Description
CVE-2021-29047	The SimpleCaptcha implementation in Liferay Portal 7.3.4, 7.3.5 and Liferay DXP 7.3 before fix pack 1 does not invalidate CAPTCHA answers after it is used, which all to repeatedly perform actions protected by a CAPTCHA challenge by reusing the same CAPTCHA answer.
CVE-2021-32918	An issue was discovered in Prosody before 0.11.9. Default settings are susceptible to remote unauthenticated denial-of-service (DoS) attacks via memory exhaustion w 5.2 or Lua 5.3.
CVE-2021-29024	In InvoicePlane 1.5.11 a misconfigured web server allows unauthenticated directory listing and file download. Allowing an attacker to directory traversal and download f private without authentication.
CVE-2021-32920	Prosody before 0.11.9 allows Uncontrolled CPU Consumption via a flood of SSL/TLS renegotiation requests.
CVE-2021-27737	Apache Traffic Server 9.0.0 is vulnerable to a remote DOS attack on the experimental Slicer plugin.
CVE-2020-21342	Insecure permissions issue in zzcms 201910 via the reset any user password in /one/getpassword.php.
CVE-2021-32572	Speco Web Viewer through 2021-05-12 allows Directory Traversal via GET request for a URI with /.. at the beginning, as demonstrated by reading the /etc/passwd file.
CVE-2021-22140	Elastic App Search versions after 7.11.0 and before 7.12.0 contain an XML External Entity Injection issue (XXE) in the App Search web crawler beta feature. Using this whose website is being crawled by App Search could craft a malicious sitemap.xml to traverse the filesystem of the host running the instance and obtain sensitive files.
CVE-2021-25693	An attacker may cause a Denial of Service (DoS) in multiple versions of Teradici PCoIP Agent via a null pointer dereference.
CVE-2020-27185	Cleartext transmission of sensitive information via Moxa Service in NPort IA5000A series serial devices. Successfully exploiting the vulnerability could enable attackers data, device configuration, and other sensitive data transmitted over Moxa Service.
CVE-2021-29747	IBM InfoSphere Information Server 11.7 could allow a remote attacker to obtain highly sensitive information due to a vulnerability in the authentication mechanism. IBM
CVE-2021-24295	It was possible to exploit an Unauthenticated Time-Based Blind SQL Injection vulnerability in the Spam protection, AntiSpam, FireWall by CleanTalk WordPress Plugin update_log function in lib/Cleantalk/ApbctWP/Firewall/SFW.php included a vulnerable query that could be injected via the User-Agent Header by manipulating the cook protection, AntiSpam, FireWall by CleanTalk WordPress plugin before 5.153.4, sending an initial request to obtain a ct_sfw_pass_key cookie and then manually setting ct_sfw_passed cookie and disallowing it from being reset.
CVE-2020-27840	A flaw was found in samba. Spaces used in a string around a domain name (DN), while supposed to be ignored, can cause invalid DN strings with spaces to instead w of-bounds memory, resulting in a crash. The highest threat from this vulnerability is to system availability.
CVE-2021-20181	A race condition flaw was found in the 9pfs server implementation of QEMU up to and including 5.2.0. This flaw allows a malicious 9p client to cause a use-after-free er escalating their privileges on the system. The highest threat from this vulnerability is to confidentiality, integrity as well as system availability.
CVE-2021-22153	A Remote Code Execution vulnerability in the Management Console component of BlackBerry UEM version(s) 12.13.1 QF2 and earlier and 12.12.1a QF6 and earlier c to potentially cause the spreadsheet application to run commands on the victim's local machine with the authority of the user.
CVE-2021-28649	An incorrect permission vulnerability in the product installer for Trend Micro HouseCall for Home Networks version 5.3.1179 and below could allow an attacker to escal arbitrary code on a specified folder and have that code be executed by an Administrator who is running a scan. Please note that an attacker must first obtain the ability privileged code on the target system to exploit this vulnerability.
CVE-2021-29591	TensorFlow is an end-to-end open source platform for machine learning. TFlite graphs must not have loops between nodes. However, this condition was not checked a craft models that would result in infinite loop during evaluation. In certain cases, the infinite loop would be replaced by stack overflow due to too many recursive calls. F implementation(https://github.com/tensorflow/tensorflow/blob/106d8f4fb89335a2c52d7c895b7a7485465ca8d9/tensorflow/lite/kernels/while.cc) could be tricked into a s body and the loop subgraphs are the same. Evaluating one of the subgraphs means calling the `Eval` function for the other and this quickly exhaust all stack space. Th TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and Please consult our security guide(https://github.com/tensorflow/tensorflow/blob/master/SECURITY.md) for more information regarding the security model and how to c and questions.
CVE-2021-31519	An incorrect permission vulnerability in the product installer folders for Trend Micro HouseCall for Home Networks version 5.3.1179 and below could allow an attacker t placing arbitrary code on a specified folder and have that code be executed by an Administrator who is running a scan. Please note that an attacker must first obtain th privileged code on the target system to exploit this vulnerability.

CVE Number	Description
CVE-2021-20202	A flaw was found in keycloak. Directories can be created prior to the Java process creating them in the temporary directory, but with wider user permissions, allowing th access to the contents that keycloak stores in this directory. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2020-12967	The lack of nested page table protection in the AMD SEV/SEV-ES feature could potentially lead to arbitrary code execution within the guest VM if a malicious administr compromise the server hypervisor.
CVE-2021-26311	In the AMD SEV/SEV-ES feature, memory can be rearranged in the guest address space that is not detected by the attestation mechanism which could be used by a m potentially lead to arbitrary code execution within the guest VM if a malicious administrator has access to compromise the server hypervisor.
CVE-2020-27833	A Zip Slip vulnerability was found in the oc binary in openshift-clients where an arbitrary file write is achieved by using a specially crafted raw container image (.tar file) symbolic links. The vulnerability is limited to the command `oc image extract`. If a symbolic link is first created pointing within the tarball, this allows further symbolic link path check. This flaw allows the tarball to create links outside the tarball's parent directory, allowing for executables or configuration files to be overwritten, resulting in a The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. Versions up to and including openshift-clients-4.7.0-202104250659 affected.
CVE-2020-24119	A heap buffer overflow read was discovered in upx 4.0.0, because the check in p_lx_elf.cpp is not perfect.
CVE-2021-29606	TensorFlow is an end-to-end open source platform for machine learning. A specially crafted TFLite model could trigger an OOB read on heap in the TFLite implementat `Split_V`(https://github.com/tensorflow/tensorflow/blob/c59c37e7b2d563967da813fa50fe20b21f4da683/tensorflow/lite/kernels/split_v.cc#L99). If `axis_value` is not a va `NumDimensions(input)`, then the `SizeOfDimension` function(https://github.com/tensorflow/tensorflow/blob/102b211d892f3abc14f845a72047809b39cc65ab/tensorflow/lite/kernels/kernel_util.h#L148-L150) will access data the tensor shape array. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and these are also affected and still in supported range.
CVE-2021-29614	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.io.decode_raw` produces incorrect results and crashes the Python ir combining `fixed_length` and wider datatypes. The implementation of the padded version(https://github.com/tensorflow/tensorflow/blob/1d8903e5b167ed0432077a3db6e462daf781d1fe/tensorflow/core/kernels/decode_padded_raw_op.cc) is buggy du pointer arithmetic rules. First, the code computes(https://github.com/tensorflow/tensorflow/blob/1d8903e5b167ed0432077a3db6e462daf781d1fe/tensorflow/core/kernels/decode_padded_raw_op.cc#L61) the element by dividing the `fixed_length` value to the size of the type argument. The `fixed_length` argument is also used to determine the size needed for the output tensor(https://github.com/tensorflow/tensorflow/blob/1d8903e5b167ed0432077a3db6e462daf781d1fe/tensorflow/core/kernels/decode_padded_raw_op.cc#L63-L79). Tl reencoding code(https://github.com/tensorflow/tensorflow/blob/1d8903e5b167ed0432077a3db6e462daf781d1fe/tensorflow/core/kernels/decode_padded_raw_op.cc#L code is the last line above: it is moving the `out_data` pointer by `fixed_length * sizeof(T)` bytes whereas it only copied at most `fixed_length` bytes from the input. This input not being decoded into the output. Furthermore, because the pointer advance is far wider than desired, this quickly leads to writing to outside the bounds of the ba write leads to interpreter crash in the reproducer mentioned here, but more severe attacks can be mounted too, given that this gadget allows writing to periodically plac The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as th and still in supported range.
CVE-2021-29605	TensorFlow is an end-to-end open source platform for machine learning. The TFLite code for allocating `TFLiteIntArray`s is vulnerable to an integer overflow issue(https://github.com/tensorflow/tensorflow/blob/4ceffae632721e52bf3501b736e4fe9d1221cdfa/tensorflow/lite/c/common.c#L24-L27). An attacker can craft a model multiplier is so large that the return value overflows the `int` datatype and becomes negative. In turn, this results in invalid value being given to `malloc`(https://github.com/tensorflow/tensorflow/blob/4ceffae632721e52bf3501b736e4fe9d1221cdfa/tensorflow/lite/c/common.c#L47-L52). In this case, `ret->size` wou invalid pointer. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorF also affected and still in supported range.
CVE-2021-31321	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Stack Based Overflow in the gray_split_cubic function of their custor library. A remote attacker might be able to overwrite Telegram's stack memory out-of-bounds on a victim device via a malicious animated sticker.
CVE-2021-31320	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Heap Buffer Overflow in the VGradientCache::generateGradientCol custom fork of the rlottie library. A remote attacker might be able to overwrite heap memory out-of-bounds on a victim device via a malicious animated sticker.
CVE-2020-36197	An improper access control vulnerability has been reported to affect earlier versions of Music Station. If exploited, this vulnerability allows attackers to compromise the s by gaining privileges, reading sensitive information, executing commands, evading detection, etc. This issue affects: QNAP Systems Inc. Music Station versions prior to versions prior to 5.2.10 on QTS 4.3.6; versions prior to 5.1.14 on QTS 4.3.3; versions prior to 5.3.16 on QuTS hero h4.5.2; versions prior to 5.3.16 on QuTScloud c4.5.4
CVE-2021-32455	SITEL CAP/PRX firmware version 5.2.01, allows an attacker with access to the device´s network to cause a denial of service condition on the device. An attacker could vulnerability by sending HTTP requests massively.
CVE-2021-25264	In multiple versions of Sophos Endpoint products for MacOS, a local attacker could execute arbitrary code with administrator privileges.
CVE-2020-36198	A command injection vulnerability has been reported to affect certain versions of Malware Remover. If exploited, this vulnerability allows remote attackers to execute ar issue affects: QNAP Systems Inc. Malware Remover versions prior to 4.6.1.0. This issue does not affect: QNAP Systems Inc. Malware Remover 3.x.

CVE Number	Description
CVE-2021-3524	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway) in versions before 14.2.21. The vulnerability is related to the injection of HTTP heade ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS reque the prior bug fix for CVE-2020-10753 did not account for the use of \r as a header separator, thus a new flaw has been created.
CVE-2020-20246	Mikrotik RouterOs stable 6.46.3 suffers from a memory corruption vulnerability in the mactel process. An authenticated remote attacker can cause a Denial of Service c access.
CVE-2020-21839	An issue was discovered in GNU LibreDWG 0.10. Crafted input will lead to an memory leak in dwg_decode_eed ../../src/decode.c:3638.
CVE-2020-20214	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from an assertion failure vulnerability in the btest process. An authenticated remote attacker can cause a Denial of Se assertion failure via a crafted packet.
CVE-2020-21835	A null pointer deference issue exists in GNU LibreDWG 0.10 via read_2004_compressed_section ../../src/decode.c:2337.
CVE-2020-21834	A null pointer deference issue exists in GNU LibreDWG 0.10 via get_bmp ../../programs/dwgbmp.c:164.
CVE-2020-20222	Mikrotik RouterOs 6.44.6 (long-term tree) suffers from a memory corruption vulnerability in the /nova/bin/sniffer process. An authenticated remote attacker can cause a (NULL pointer dereference).
CVE-2020-20236	Mikrotik RouterOs 6.46.3 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/sniffer process. An authenticated remote attacker can cause a Der improper memory access.
CVE-2021-24324	The 404 SEO Redirection WordPress plugin through 1.3 is lacking CSRF checks in all its settings, allowing attackers to make a logged in user change the plugin's setti sanitisation and escaping in some fields, it could also lead to Stored Cross-Site Scripting issues
CVE-2020-20245	Mikrotik RouterOs stable 6.46.3 suffers from a memory corruption vulnerability in the log process. An authenticated remote attacker can cause a Denial of Service due access.
CVE-2021-32925	admin/user_import.php in Chamilo 1.11.x reads XML data without disabling the ability to load external entities.
CVE-2020-25713	A malformed input file can lead to a segfault due to an out of bounds array access in raptor_xml_writer_start_element_common.
CVE-2020-20237	Mikrotik RouterOs 6.46.3 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/sniffer process. An authenticated remote attacker can cause a Der improper memory access.
CVE-2020-21817	A null pointer dereference issue exists in GNU LibreDWG 0.10.2641 via htmlescape ../../programs/escape.c:29. which causes a denial of service (application crash).
CVE-2020-21815	A null pointer deference issue exists in GNU LibreDWG 0.10.2641 via output_TEXT ../../programs/dwg2SVG.c:114, which causes a denial of service (application crash)
CVE-2020-20220	Mikrotik RouterOs prior to stable 6.47 suffers from a memory corruption vulnerability in the /nova/bin/bfd process. An authenticated remote attacker can cause a Denial pointer dereference).
CVE-2021-32456	SITEL CAP/PRX firmware version 5.2.01 allows an attacker with access to the local network of the device to obtain the authentication passwords by analysing the netw
CVE-2020-20227	Mikrotik RouterOs stable 6.47 suffers from a memory corruption vulnerability in the /nova/bin/diskd process. An authenticated remote attacker can cause a Denial of Se memory access.
CVE-2021-22139	Kibana versions before 7.12.1 contain a denial of service vulnerability was found in the webhook actions due to a lack of timeout or a limit on the request size. An attacl create webhook actions could drain the Kibana host connection pool, making Kibana unavailable for all other users.

CVE Number	Description
CVE-2007-5967	A flaw in Mozilla's embedded certificate code might allow web sites to install root certificates on devices without user approval.
CVE-2021-32453	SITEL CAP/PRX firmware version 5.2.01 allows an attacker with access to the local network, to access via HTTP to the internal configuration database of the device wi authentication. An attacker could exploit this vulnerability in order to obtain information about the device´s configuration.
CVE-2021-29511	evm is a pure Rust implementation of Ethereum Virtual Machine. Prior to the patch, when executing specific EVM opcodes related to memory operations that use `evm_core::Memory::copy_large`, the `evm` crate can over-allocate memory when it is not needed, making it possible for an attacker to perform denial-of-service attacl corrected in commit `19ade85`. Users should upgrade to `==0.21.1, ==0.23.1, ==0.24.1, ==0.25.1, >=0.26.1`. There are no workarounds. Please upgrade your `evm` cr
CVE-2021-31876	Bitcoin Core 0.12.0 through 0.21.1 does not properly implement the replacement policy specified in BIP125, which makes it easier for attackers to trigger a loss of funds attack against downstream projects such as Lightning network nodes. An unconfirmed child transaction with nSequence = 0xff_ff_ff_ff, spending an unconfirmed parent 0xff_ff_ff_fd, should be replaceable because there is inherited signaling by the child transaction. However, the actual PreChecks implementation does not enforce this. rejects the replacement attempt of the unconfirmed child transaction.
CVE-2021-24279	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, low level users, such as subscribers, could use the import_from_debug AJAX action to install any WordPress repository.
CVE-2021-29041	Denial-of-service (DoS) vulnerability in the Multi-Factor Authentication module in Liferay DXP 7.3 before fix pack 1 allows remote authenticated attackers to prevent any authenticating by (1) enabling Time-based One-time password (TOTP) on behalf of the other user or (2) modifying the other user's TOTP shared secret.
CVE-2021-32816	ProtonMail Web Client is the official AngularJS web client for the ProtonMail secure email service. ProtonMail Web Client before version 3.16.60 has a regular expressi vulnerability. This was fixed in commit 6687fb. There is a full report available in the referenced GHSL-2021-027.
CVE-2020-20253	Mikrotik RouterOs before 6.47 (stable tree) suffers from a divison by zero vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause a D a divide by zero error.
CVE-2020-23995	An information disclosure vulnerability in ILIAS before 5.3.19, 5.4.12 and 6.0 allows remote authenticated attackers to get the upload data path via a workspace upload.
CVE-2021-29506	GraphHopper is an open-source Java routing engine. In GrassHopper from version 2.0 and before version 2.4, there is a regular expression injection vulnerability that r Service. This has been patched in 2.4 and 3.0 See this pull request for the fix: https://github.com/graphhopper/graphhopper/pull/2304
CVE-2020-20254	Mikrotik RouterOs before 6.47 (stable tree) suffers from a memory corruption vulnerability in the /nova/bin/lcdstat process. An authenticated remote attacker can cause (NULL pointer dereference).
CVE-2020-27149	By exploiting a vulnerability in NPort IA5150A/IA5250A Series before version 1.5, a user with “Read Only” privilege level can send requests via the web console to have configuration changed.
CVE-2021-23909	An issue was discovered in HERMES 2.1 in the MBUX Infotainment System on Mercedes-Benz vehicles through 2021. The SH2 MCU allows remote code execution.
CVE-2021-24282	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, any authenticated user, such as a subscriber, could use the various AJAX actions in the plugin to For example, an attacker could use wpcf7r_reset_settings to reset the plugin’s settings, wpcf7r_add_action to add actions to a form, and more.
CVE-2021-29601	TensorFlow is an end-to-end open source platform for machine learning. The TFLite implementation of concatenation is vulnerable to an integer overflow issue(https://github.com/tensorflow/tensorflow/blob/7b7352a724b690b11bfaae2cd54bc3907daf6285/tensorflow/lite/kernels/concatenation.cc#L70-L76). An attacker car that the dimensions of one of the concatenation input overflow the values of `int`. TFLite uses `int` to represent tensor dimensions, whereas TF uses `int64`. Hence, val trigger an integer overflow when converted to TFLite format. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, Tens TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29613	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `tf.raw_ops.CTCLoss` allows an attacker to trigger an OOB read from included in TensorFlow 2.5.0. We will also cherrypick these commits on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are als supported range.
CVE-2021-30213	Knowage Suite 7.3 is vulnerable to unauthenticated reflected cross-site scripting (XSS). An attacker can inject arbitrary web script in '/servlet/AdapterHTTP' via the 'targ
CVE-2020-19274	A Cross SIte Scripting (XSS) vulnerability exists in Dhcms 2017-09-18 in guestbook via the message board, which could let a remote malicious user execute arbitrary c

CVE Number	Description
CVE-2021-24325	The tab parameter of the settings page of the 404 SEO Redirection WordPress plugin through 1.3 is vulnerable to a reflected Cross-Site Scripting (XSS) issue as user i sanitised or escaped before being output in an attribute.
CVE-2021-3457	An improper authorization handling flaw was found in Foreman. The Shellhooks plugin for the smart-proxy allows Foreman clients to execute actions that should be limi Server. This flaw allows an authenticated local attacker to access and delete limited resources and also causes a denial of service on the Foreman server. The highest vulnerability is to integrity and system availability.
CVE-2021-32054	Firely/Incendi Spark before 1.5.5-r4 lacks Content-Disposition headers in certain situations, which may cause crafted files to be delivered to clients such that they are re victim's web browser.
CVE-2021-29046	Cross-site scripting (XSS) vulnerability in the Asset module's category selector input field in Liferay Portal 7.3.5 and Liferay DXP 7.3 before fix pack 1, allows remote att arbitrary web script or HTML via the _com_liferay_asset_categories_admin_web_portlet_AssetCategoriesAdminPortlet_title parameter.
CVE-2021-24299	The ReDi Restaurant Reservation WordPress plugin before 21.0426 provides the functionality to let users make restaurant reservations. These reservations are stored 'Upcoming' page provided by the plugin. An unauthenticated user can fill in the form to make a restaurant reservation. The form to make a restaurant reservation field c not use proper input validation and can be used to store XSS payloads. The XSS payloads will be executed when the plugin user goes to the 'Upcoming' page, which is https://upcoming.reservationdiary.eu/ loaded in an iframe, and the stored reservation with XSS payload is loaded.
CVE-2021-24290	There are several endpoints in the Store Locator Plus for WordPress plugin through 5.5.15 that could allow unauthenticated attackers the ability to inject malicious Java
CVE-2021-29045	Cross-site scripting (XSS) vulnerability in the Redirect module's redirection administration page in Liferay Portal 7.3.2 through 7.3.5, and Liferay DXP 7.3 before fix pacl attackers to inject arbitrary web script or HTML via the _com_liferay_redirect_web_internal_portlet_RedirectPortlet_destinationURL parameter.
CVE-2021-24288	When subscribing using AcyMailing, the 'redirect' parameter isn't properly sanitized. Turning the request from POST to GET, an attacker can craft a link containing a po landing page and send it to the victim.
CVE-2019-14827	A vulnerability was found in Moodle where javaScript injection was possible in some Mustache templates via recursive rendering from contexts. Mustache helper tags tl template contexts were not being escaped before that context was injected into another Mustache helper, which could result in script injection in some templates. This a 3.7.1, 3.6 to 3.6.5, 3.5 to 3.5.7 and earlier unsupported versions.
CVE-2021-29051	Cross-site scripting (XSS) vulnerability in the Asset module's Asset Publisher app in Liferay Portal 7.2.1 through 7.3.5, and Liferay DXP 7.1 before fix pack 21, 7.2 befo before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_asset_publisher_web_portlet_AssetPublisherPortlet_INSTANCE_XXXXXXXXXXXX_assetEntryId parameter.
CVE-2021-29048	Cross-site scripting (XSS) vulnerability in the Layout module's page administration page in Liferay Portal 7.3.4, 7.3.5 and Liferay DXP 7.2 before fix pack 11 and 7.3 bef remote attackers to inject arbitrary web script or HTML via the _com_liferay_layout_admin_web_portlet_GroupPagesPortlet_name parameter.
CVE-2021-29044	Cross-site scripting (XSS) vulnerability in the Site module's membership request administration pages in Liferay Portal 7.0.0 through 7.3.5, and Liferay DXP 7.0 before f fix pack 21, 7.2 before fix pack 10 and 7.3 before fix pack 1 allows remote attackers to inject arbitrary web script or HTML via the _com_liferay_site_my_sites_web_portlet_MySitesPortlet_comments parameter.
CVE-2021-29039	Cross-site scripting (XSS) vulnerability in the Asset module's categories administration page in Liferay Portal 7.3.4 allows remote attackers to inject arbitrary web script name.
CVE-2021-24286	The settings page of the Redirect 404 to parent WordPress plugin before 1.3.1 did not properly sanitise the tab parameter before outputting it back, leading to a reflecte issue
CVE-2021-33041	vmd through 1.34.0 allows 'div class="markdown-body"' XSS, as demonstrated by Electron remote code execution via require('child_process').execSync('calc.exe') on ' attack on macOS.
CVE-2021-20392	IBM QRadar User Behavior Analytics 1.0.0 through 4.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the W intended functionality potentially leading to credentials disclosure within a trusted session.
CVE-2021-24287	The settings page of the Select All Categories and Taxonomies, Change Checkbox to Radio Buttons WordPress plugin before 1.3.2 did not properly sanitise the tab pa outputting it back, leading to a reflected Cross-Site Scripting issue
CVE-2020-17891	TP-Link Archer C1200 firmware version 1.13 Build 2018/01/24 rel.52299 EU has a XSS vulnerability allowing a remote attacker to execute arbitrary code.
CVE-2019-10062	The HTMLSanitizer class in html-sanitizer.ts in all released versions of the Aurelia framework 1.x repository is vulnerable to XSS. The sanitizer only attempts to filter SC makes it feasible for remote attackers to conduct XSS attacks via (for example) JavaScript code in an attribute of various other elements. An attacker might also exploit SCRIPT string is processed by splitting and nesting them for example.

CVE Number	Description
CVE-2020-18194	Cross Site Scripting (XSS) in emlog v6.0.0 allows remote attackers to execute arbitrary code by adding a crafted script as a link to a new blog post.
CVE-2020-29205	XSS in signup form in Project Worlds Online Examination System 1.0 allows remote attacker to inject arbitrary code via the name field
CVE-2020-24026	TinyShop, a free and open source mall based on RageFrame2, has a stored XSS vulnerability that affects version 1.2.0. TinyShop allows XSS via the explain_first and parameters of the /evaluate/index.php page. The vulnerability may be exploited remotely, resulting in cross-site scripting (XSS) or information disclosure.
CVE-2021-24291	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery WordPress plugin before 1.5.69 was vulnerable to Reflected Cross-Site Scripting (XSS) issues via the ga and _id GET parameters passed to the bwg_frontend_data AJAX action (available to both unauthenticated and authenticated users)
CVE-2021-20221	An out-of-bounds heap buffer access issue was found in the ARM Generic Interrupt Controller emulator of QEMU up to and including qemu 4.2.0on aarch64 platform. T because while writing an interrupt ID to the controller memory area, it is not masked to be 4 bits wide. It may lead to the said issue while updating controller state fields processing. A privileged guest user may use this flaw to crash the QEMU process on the host resulting in DoS scenario.
CVE-2021-3537	A vulnerability found in libxml2 in versions before 2.9.11 shows that it did not propagate errors while parsing XML mixed content, causing a NULL dereference. If an unt was parsed in recovery mode and post-validated, the flaw could be used to crash the application. The highest threat from this vulnerability is to system availability.
CVE-2020-27184	The NPort IA5000A Series devices use Telnet as one of the network device management services. Telnet does not support the encryption of client-server communicati vulnerable to Man-in-the-Middle attacks.
CVE-2021-29043	The Portal Store module in Liferay Portal 7.0.0 through 7.3.5, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 21, 7.2 before fix pack 10 and 7.3 before fix pa obfuscate the S3 store's proxy password, which allows attackers to steal the proxy password via man-in-the-middle attacks or shoulder surfing.
CVE-2021-32921	An issue was discovered in Prosody before 0.11.9. It does not use a constant-time algorithm for comparing certain secret strings when running under Lua 5.2 or later. T used in a timing attack to reveal the contents of secret strings to an attacker.
CVE-2021-27342	An authentication brute-force protection mechanism bypass in telnetd in D-Link Router model DIR-842 firmware version 3.0.2 allows a remote attacker to circumvent th down delay period via a timing-based side-channel attack
CVE-2021-23135	Exposure of System Data to an Unauthorized Control Sphere vulnerability in web UI of Argo CD allows attacker to cause leaked secret data into web UI error message affects Argo CD 1.8 versions prior to 1.8.7; 1.7 versions prior to 1.7.14.
CVE-2021-20564	IBM Cloud Pak for Security (CP4S) 1.4.0.0, 1.5.0.0, 1.5.0.1, 1.6.0.0, and 1.6.0.1 could allow a remote attacker to obtain sensitive information, caused by the failure to p Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 199235.
CVE-2021-32613	In radare2 through 5.3.0 there is a double free vulnerability in the pyc parse via a crafted file which can lead to DoS.
CVE-2021-31319	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by an Integer Overflow in the LOTGradient::populate function of their cus library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker.
CVE-2021-31318	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Type Confusion in the LOTCompLayerItem::LOTCompLayerItem fur fork of the rlottie library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker.
CVE-2020-23851	A stack-based buffer overflow vulnerability exists in ffjpeg through 2020-07-02 in the jfif_decode(void *ctxt, BMP *pb) function at ffjpeg/src/jfif.c:513:28, which could cau by submitting a malicious jpeg image.
CVE-2021-31322	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Heap Buffer Overflow in the LOTGradient::populate function of their rlottie library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker.
CVE-2020-23856	Use-after-Free vulnerability in cflow 1.6 in the void call(char *name, int line) function at src/parser.c, which could cause a denial of service via the pointer variable caller·
CVE-2020-23852	A heap based buffer overflow vulnerability exists in ffjpeg through 2020-07-02 in the jfif_decode(void *ctxt, BMP *pb) function at ffjpeg/src/jfif.c (line 544 & line 545), whi of service by submitting a malicious jpeg image.

CVE Number	Description
CVE-2020-23861	A heap-based buffer overflow vulnerability exists in LibreDWG 0.10.1 via the read_system_page function at libredwg-0.10.1/src/decode_r2007.c:666:5, which causes a submitting a dwg file.
CVE-2021-31315	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Stack Based Overflow in the blit function of their custom fork of the r attacker might be able to access Telegram's stack memory out-of-bounds on a victim device via a malicious animated sticker.
CVE-2020-27824	A flaw was found in OpenJPEG's encoder in the opj_dwt_calc_explicit_stepsizes() function. This flaw allows an attacker who can supply crafted input to decomposition overflow. The highest threat from this vulnerability is to system availability.
CVE-2020-27830	A vulnerability was found in Linux Kernel where in the spk_ttyio_receive_buf2() function, it would dereference spk_ttyio_synth without checking whether it is NULL or nc NULL-ptr deref crash.
CVE-2021-31323	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Heap Buffer Overflow in the LottieParserImpl::parseDashProperty fu fork of the rlottie library. A remote attacker might be able to access heap memory out-of-bounds on a victim device via a malicious animated sticker.
CVE-2021-31317	Telegram Android <7.1.0 (2090), Telegram iOS <7.1, and Telegram macOS <7.1 are affected by a Type Confusion in the VDasher constructor of their custom fork of th remote attacker might be able to access Telegram's heap memory out-of-bounds on a victim device via a malicious animated sticker.
CVE-2021-22152	A Denial of Service due to Improper Input Validation vulnerability in the Management Console component of BlackBerry UEM version(s) 12.13.1 QF2 and earlier and 12 could allow an attacker to potentially to prevent any new user connections.
CVE-2021-30211	Knowage Suite 7.3 is vulnerable to Stored Cross-Site Scripting (XSS). An attacker can inject arbitrary web script in '/knowage/restful-services/signup/update' via the 'su
CVE-2021-30212	Knowage Suite 7.3 is vulnerable to Stored Cross-Site Scripting (XSS). An attacker can inject arbitrary web script in '/knowage/restful-services/documentnotes/saveNote parameter.
CVE-2021-23384	The package koa-remove-trailing-slashes before 2.0.2 are vulnerable to Open Redirect via the use of trailing double slashes in the URL when accessing the vulnerable https://example.com//attacker.example/). The vulnerable code is in index.js::removeTrailingSlashes(), as the web server uses relative URLs instead of absolute URLs.
CVE-2021-24326	The tab parameter of the settings page of the All 404 Redirect to Homepage WordPress plugin before 1.21 was vulnerable to an authenticated reflected Cross-Site Scri user input was not properly sanitised before being output in an attribute.
CVE-2021-24283	The tab GET parameter of the settings page is not sanitised or escaped when being output back in an HTML attribute, leading to a reflected XSS issue.
CVE-2020-19924	In Boostnote 0.12.1, exporting to PDF contains opportunities for XSS attacks.
CVE-2020-24992	There is a cross site scripting vulnerability on CmsWing 1.3.7. This vulnerability (stored XSS) is triggered when an administrator accesses the content management mo
CVE-2021-32817	express-hbs is an Express handlebars template engine. express-hbs mixes pure template data with engine configuration options through the Express render API. More parameter may trigger file disclosure vulnerabilities in downstream applications. This potential vulnerability is somewhat restricted in that only files with existing extentio can be included, files that lack an extension will have .hbs appended to them. For complete details refer to the referenced GHSL-2021-019 report. Notes in documentat help users of express-hbs avoid this potential information exposure vulnerability.
CVE-2020-24993	There is a cross site scripting vulnerability on CmsWing 1.3.7. This vulnerability (stored XSS) is triggered when visitors access the article module.
CVE-2021-24277	The RSS for Yandex Turbo WordPress plugin before 1.30 did not properly sanitise the user inputs from its Счетчики settings tab before outputting them back in the pa authenticated stored Cross-Site Scripting issues
CVE-2020-28722	Deskpro Cloud Platform and on-premise 2020.2.3.48207 from 2020-07-30 contains a cross-site scripting (XSS) vulnerability that can lead to an account takeover via cu
CVE-2021-30214	Knowage Suite 7.3 is vulnerable to Stored Client-Side Template Injection in '/knowage/restful-services/signup/update' via the 'name' parameter.

CVE Number	Description
CVE-2021-24292	The Happy Addons for Elementor WordPress plugin before 2.24.0, Happy Addons Pro for Elementor WordPress plugin before 1.17.0 have a number of widgets that ar Cross-Site Scripting(XSS) by lower-privileged users such as contributors, all via a similar method: The “Card” widget accepts a “title_tag” parameter. Although the elem set of possible html tags, it is possible to send a ‘save_builder’ request with the “heading_tag” set to “script”, and the actual “title” parameter set to JavaScript to be exe tags added by the “heading_tag” parameter.
CVE-2020-16632	A XSS Vulnerability in /uploads/dede/action_search.php in DedeCMS V5.7 SP2 allows an authenticated user to execute remote arbitrary code via the keyword parame
CVE-2021-20535	IBM Jazz Reporting Service 6.0.6.1, 7.0, 7.0.1, and 7.0.2 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauth system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 198834.
CVE-2021-3531	A flaw was found in the Red Hat Ceph Storage RGW in versions before 14.2.21. When processing a GET Request for a swift URL that ends with two slashes it can cau resulting in a denial of service. The greatest threat to the system is of availability.
CVE-2021-29023	InvoicePlane 1.5.11 doesn't have any rate-limiting for password reset and the reset token is generated using a weak mechanism that is predictable.
CVE-2021-29040	The JSON web services in Liferay Portal 7.3.4 and earlier, and Liferay DXP 7.0 before fix pack 97, 7.1 before fix pack 20 and 7.2 before fix pack 10 may provide overly messages, which allows remote attackers to use the contents of error messages to help launch another, more focused attacks via crafted inputs.
CVE-2021-29609	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `SparseAdd` results in allowing attackers to exploit undefined behavio pointers) as well as write outside of bounds of heap allocated data. The implementation(https://github.com/tensorflow/tensorflow/blob/656e7673b14acd7835dc778867f84916c6d1cac2/tensorflow/core/kernels/sparse_add_op.cc) has a large two sparse tensor inputs (6 tensors in total), but does not validate that the tensors are not empty or that the second dimension of `*_indices` matches the size of corres allows attackers to send tensor triples that represent invalid sparse tensors to abuse code assumptions that are not protected by validation. The fix will be included in T will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range
CVE-2021-29608	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.RaggedTensorToTensor`, an attacker can exploit an ur input arguments are empty. The implementation(https://github.com/tensorflow/tensorflow/blob/656e7673b14acd7835dc778867f84916c6d1cac2/tensorflow/core/kernels/ragged_tensor_to_tensor_op.cc checks that one of the tensors is not empty, but does not check for the other ones. There are multiple `DCHECK` validations to prevent heap OOB, but these are no-op hence they don't prevent anything. The fix will be included in TensorFlow 2.5.0. We will also cherrypick these commits on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorF TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29607	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `SparseAdd` results in allowing attackers to exploit undefined behavio pointers) as well as write outside of bounds of heap allocated data. The implementation(https://github.com/tensorflow/tensorflow/blob/656e7673b14acd7835dc778867f84916c6d1cac2/tensorflow/core/kernels/sparse_sparse_binary_op_shar validation for the two sparse tensor inputs (6 tensors in total), but does not validate that the tensors are not empty or that the second dimension of `*_indices` matches corresponding `*_shape`. This allows attackers to send tensor triples that represent invalid sparse tensors to abuse code assumptions that are not protected by validati included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also a supported range.
CVE-2020-13667	Access bypass vulnerability in of Drupal Core Workspaces allows an attacker to access data without correct permissions. The Workspaces module doesn't sufficiently permissions when switching workspaces, leading to an access bypass vulnerability. An attacker might be able to see content before the site owner intends people to se vulnerability is mitigated by the fact that sites are only vulnerable if they have installed the experimental Workspaces module. This issue affects Drupal Core8.8.X versi 8.9.X versions prior to 8.9.6; 9.0.X versions prior to 9.0.6.
CVE-2020-36289	Affected versions of Atlassian Jira Server and Data Center allow an unauthenticated user to enumerate users via an Information Disclosure vulnerability in the QueryComponentRendererValue!Default.jspa endpoint. The affected versions are before version 8.5.13, from version 8.6.0 before 8.13.5, and from version 8.14.0 befo
CVE-2021-20565	IBM Cloud Pak for Security (CP4S) 1.4.0.0, 1.5.0.0, 1.5.0.1, 1.6.0.0, and 1.6.0.1 uses a protection mechanism that relies on the existence or values of an input, but the by an untrusted actor in a way that bypasses the protection mechanism. IBM X-Force ID: 199236.
CVE-2021-20995	In multiple managed switches by WAGO in different versions the webserver cookies of the web based UI contain user credentials.
CVE-2021-23910	An issue was discovered in HERMES 2.1 in the MBUX Infotainment System on Mercedes-Benz vehicles through 2021. There is an out-of-bounds array access in Rem
CVE-2021-22137	In Elasticsearch versions before 7.11.2 and 6.8.15 a document disclosure flaw was found when Document or Field Level Security is used. Search queries do not prope permissions when executing certain cross-cluster search queries. This could result in the search disclosing the existence of documents the attacker should not be able result in an attacker gaining additional insight into potentially sensitive indices.
CVE-2021-20429	IBM QRadar User Behavior Analytics 1.0.0 through 4.1.0 could disclose sensitive information due an overly permissive cross-domain policy. IBM X-Force ID: 196334.

CVE Number	Description
CVE-2021-22135	Elasticsearch versions before 7.11.2 and 6.8.15 contain a document disclosure flaw was found in the Elasticsearch suggester and profile API when Document and Fiel enabled. The suggester and profile API are normally disabled for an index when document level security is enabled on the index. Certain queries are able to enable the which could lead to disclosing the existence of documents and fields the attacker should not be able to view.
CVE-2021-32917	An issue was discovered in Prosody before 0.11.9. The proxy65 component allows open access by default, even if neither of the users has an XMPP account on the lo unrestricted use of the server's bandwidth.
CVE-2021-21424	Symfony is a PHP framework for web and console applications and a set of reusable PHP components. The ability to enumerate users was possible without relevant pe different handling depending on whether the user existed or not when attempting to use the switch users functionality. We now ensure that 403s are returned whether t user cannot switch to a user or if the user does not exist. The patch for this issue is available for branch 3.4.
CVE-2021-20996	In multiple managed switches by WAGO in different versions special crafted requests can lead to cookies being transferred to third parties.
CVE-2021-20993	In multiple managed switches by WAGO in different versions the activated directory listing provides an attacker with the index of the resources located inside the direct
CVE-2019-19276	A vulnerability has been identified in SIMATIC HMI Comfort Panels 1st Generation (incl. SIPLUS variants) (All versions < V16 Update 4), SIMATIC HMI KTP Mobile Pa Update 4). Specially crafted packets sent to port 161/udp can cause the SNMP service of affected devices to crash. A manual restart of the device is required to resum service.
CVE-2020-12526	TwinCAT OPC UA Server in versions up to 2.3.0.12 and IPC Diagnostics UA Server in versions up to 3.1.0.1 from Beckhoff Automation GmbH & Co. KG are vulnerable attacks. The attacker needs to send several specifically crafted requests to the running OPC UA server. After some of these requests the OPC UA server is no longer r This is without effect to the real-time functionality of IPCs.
CVE-2021-22154	An Information Disclosure vulnerability in the Management Console component of BlackBerry UEM version(s) 12.13.1 QF2 and earlier and 12.12.1a QF6 and earlier cc potentially gain access to a victim's web history.
CVE-2020-19275	An Information Disclosure vulnerability exists in dhcms 2017-09-18 when entering invalid characters after the normal interface, which causes an error that will leak the p
CVE-2021-24315	The GiveWP – Donation Plugin and Fundraising Platform WordPress plugin before 2.10.4 did not sanitise or escape the Background Image field of its Stripe Checkout in its Email settings, leading to authenticated (admin+) Stored XSS issues.
CVE-2020-23689	In YFCMF v2.3.1, there is a stored XSS vulnerability in the comments section of the news page.
CVE-2020-18167	Cross Site Scripting (XSS) in LAOBANCMS v2.0 allows remote attackers to execute arbitrary code by injecting commands into the "Homepage Introduction" field of cor "admin/info.php?shuyu".
CVE-2021-24327	The SEO Redirection Plugin – 301 Redirect Manager WordPress plugin before 6.4 did not sanitise the Redirect From and Redirect To fields when creating a new redire allowing high privilege users (even with the unfiltered_html disabled) to set XSS payloads
CVE-2021-24323	When taxes are enabled, the "Additional tax classes" field was not properly sanitised or escaped before being output back in the admin dashboard, allowing high privile to use XSS payloads even when the unfiltered_html is disabled
CVE-2020-18165	Cross Site Scripting (XSS) in LAOBANCMS v2.0 allows remote attackers to execute arbitrary code by injecting commands into the "Website SEO Keywords" field on th "admin/info.php?shuyu".
CVE-2021-32617	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An inefficient algorithm (quadratic complexity) w versions v0.27.3 and earlier. The inefficient algorithm is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the a denial of service, if they can trick the victim into running Exiv2 on a crafted image file. The bug is fixed in version v0.27.4. Note that this bug is only triggered when _w which is a less frequently used Exiv2 operation than _reading_ the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add a argument such as `rm`.
CVE-2021-29571	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of bou data if attacker supplies specially crafted inputs. The implementation(https://github.com/tensorflow/tensorflow/blob/31bd5026304677faa8a0b77602c6154171b9aec1/tensorflow/core/kernels/image/draw_bounding_box_op. assumes that the last element of `boxes` input is 4, as required by [the op](https://www.tensorflow.org/api_docs/python/tf/raw_ops/DrawBoundingBoxesV2). Since this i attackers passing values less than 4 can write outside of bounds of heap allocated objects and cause memory corruption. If the last dimension in `boxes` is less than 4, `tboxes(b, bb, 3)` will access data outside of bounds. Further during code execution there are also writes to these indices. The fix will be included in TensorFlow 2.5.0. this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-29592	TensorFlow is an end-to-end open source platform for machine learning. The fix for CVE-2020-15209(https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1520 when the target shape of `Reshape` operator is given by the elements of a 1-D tensor. As such, the fix for the vulnerability(https://github.com/tensorflow/tensorflow/blob/9c1dc920d8ffb4893d6c9d27d1f039607b326743/tensorflow/lite/core/subgraph.cc#L1062-L1074) allowed pass backed tensor with a 1D shape. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2 2.1.4, as these are also affected and still in supported range.
CVE-2021-31341	Uploading a table mapping using a manipulated XML file results in an exception that could expose information about the application-server and the used XML-framewo Database Replication Module (All versions prior to v7.0.1).
CVE-2021-31339	A vulnerability has been identified in Mendix Excel Importer Module (All versions < V9.0.3). Uploading a manipulated XML File results in an exception that could expose Application-Server and the used XML-Framework.
CVE-2021-29052	The Data Engine module in Liferay Portal 7.3.0 through 7.3.5, and Liferay DXP 7.3 before fix pack 1 does not check permissions in DataDefinitionResourceImpl.getSiteDataDefinitionByContentTypeByDataDefinitionKey, which allows remote authenticated users to view DDMStructures via GET API c
CVE-2020-24740	An issue was discovered in Pluck 4.7.10-dev2. There is a CSRF vulnerability that can editpage via a /admin.php?action=editpage
CVE-2021-20250	A flaw was found in wildfly. The JBoss EJB client has publicly accessible privileged actions which may lead to information disclosure on the server it is deployed on. Th this vulnerability is to data confidentiality.
CVE-2021-24281	In the Redirection for Contact Form 7 WordPress plugin before 2.3.4, any authenticated user, such as a subscriber, could use the delete_action_post AJAX action to de target site.
CVE-2021-32622	Matrix-React-SDK is a react-based SDK for inserting a Matrix chat/voip client into a web page. Before version 3.21.0, when uploading a file, the local file preview can le scripts embedded in the uploaded file. This can only occur after several user interactions to open the preview in a separate tab. This only impacts the local user while ir uploading. It cannot be exploited remotely or by other users. This vulnerability is patched in version 3.21.0.
CVE-2021-20331	Specific versions of the MongoDB C# Driver may erroneously publish events containing authentication-related data to a command listener configured by an application. may contain security-sensitive data when commands such as "saslStart", "saslContinue", "isMaster", "createUser", and "updateUser" are executed. Without due care, a inadvertently expose this authenticated-related information, e.g., by writing it to a log file. This issue only arises if an application enables the command listener feature (default). This issue affects the MongoDB C# Driver v2.12 versions prior to and including 2.12.1.
CVE-2020-15279	An Improper Access Control vulnerability in the logging component of Bitdefender Endpoint Security Tools for Windows versions prior to 6.6.23.320 allows a regular us exclusion paths. This issue was discovered during external security research.
CVE-2021-22138	In Logstash versions after 6.4.0 and before 6.8.15 and 7.12.0 a TLS certificate validation flaw was found in the monitoring feature. When specifying a trusted server CA would not properly verify the certificate returned by the monitoring server. This could result in a man in the middle style attack against the Logstash monitoring data.
CVE-2021-29623	Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata. A read of uninitialized memory was found v0.27.3 and earlier. Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. The read of uninitialized me Exiv2 is used to read the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to leak a few bytes of stack memory, if they can trick the Exiv2 on a crafted image file. The bug is fixed in version v0.27.4.
CVE-2021-29612	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a heap buffer overflow in Eigen implementation of `tf.raw_ops.Banded implementation(https://github.com/tensorflow/tensorflow/blob/eccb7ec454e6617738554a255d77f08e60ee0808/tensorflow/core/kernels/linalg/banded_triangular_solve_ `ValidateInputTensors` for input validation but fails to validate that the two tensors are not empty. Furthermore, since `OP_REQUIRES` macro only stops execution of c setting `ctx->status()` to a non-OK value, callers of helper functions that use `OP_REQUIRES` must check value of `ctx->status()` before continuing. This doesn't happ implementation(https://github.com/tensorflow/tensorflow/blob/eccb7ec454e6617738554a255d77f08e60ee0808/tensorflow/core/kernels/linalg/banded_triangular_solve_ validation that is present is also not effective. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, T TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29611	TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `SparseReshape` results in a denial of service based on a `CHECK`-f implementation(https://github.com/tensorflow/tensorflow/blob/e87b51ce05c3eb172065a6ea5f48415854223285/tensorflow/core/kernels/sparse_reshape_op.cc#L40) ha input arguments specify a valid sparse tensor. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 and TensorFlow 2. only affected versions.
CVE-2021-29610	TensorFlow is an end-to-end open source platform for machine learning. The validation in `tf.raw_ops.QuantizeAndDequantizeV2` allows invalid values for `axis` argum validation(https://github.com/tensorflow/tensorflow/blob/eccb7ec454e6617738554a255d77f08e60ee0808/tensorflow/core/kernels/quantize_and_dequantize_op.cc#L74 two different conditions. If `axis_ < -1` the condition in `OP_REQUIRES` will still be true, but this value of `axis_` results in heap underflow. This allows attackers to read the heap. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2 affected and still in supported range.
CVE-2021-22136	In Kibana versions before 7.12.0 and 6.8.15 a flaw in the session timeout was discovered where the xpack.security.session.idleTimeout setting is not being respected. background polling activities unintentionally extending authenticated users sessions, preventing a user session from timing out.

CVE Number	Description
CVE-2021-29510	Pydantic is a data validation and settings management using Python type hinting. In affected versions passing either `'infinity'`, `'inf'` or `float('inf')` (or their negatives) to fields causes validation to run forever with 100% CPU usage (on one CPU). Pydantic has been patched with fixes available in the following versions: v1.8.2, v1.7.4, v1. are available on pypi(https://pypi.org/project/pydantic/#history), and will be available on conda-forge(https://anaconda.org/conda-forge/pydantic) soon. See the changel docs.helpmanual.io/) for details. If you absolutely can't upgrade, you can work around this risk using a validator(https://pydantic-docs.helpmanual.io/usage/validators/) t This is not an ideal solution (in particular you'll need a slightly different function for datetimes), instead of a hack like this you should upgrade pydantic. If you are not usi v1.6.x and are unable to upgrade to a fixed version of pydantic, please create an issue at https://github.com/samuelcolvin/pydantic/issues requesting a back-port, and w release a patch for earlier versions of pydantic.
CVE-2021-20391	IBM QRadar User Behavior Analytics 1.0.0 through 4.1.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 195
CVE-2021-3200	Buffer overflow vulnerability in libsolv 2020-12-13 via the Solver * testcase_read(Pool *pool, FILE *fp, const char *testcase, Queue *job, char **resultp, int *resultflagsp src/testcase.c: line 2334, which could cause a denial of service
CVE-2020-14354	A possible use-after-free and double-free in c-ares lib version 1.16.0 if ares_destroy() is called prior to ares_getaddrinfo() completing. This flaw possibly allows an attac that uses c-ares lib. The highest threat from this vulnerability is to this service availability.
CVE-2020-27769	In ImageMagick versions before 7.0.9-0, there are outside the range of representable values of type 'float' at MagickCore/quantize.c.
CVE-2021-32618	The Python "Flask-Security-Too" package is used for adding security features to your Flask application. It is an is an independently maintained version of Flask-Securit version of Flask-Security. All versions of Flask-Security-Too allow redirects after many successful views (e.g. /login) by honoring the ?next query param. There is code the url specified in the next parameter is either relative OR has the same netloc (network location) as the requesting URL. This check utilizes Pythons urlsplit library. Ho are very lenient on the kind of URL they accept and 'fill in the blanks' when presented with a possibly incomplete URL. As a concrete example - setting http://login?next FS's relative URL check however many browsers will gladly convert this to http://github.com. Thus an attacker could send such a link to an unwitting user, using a legiti redirect to whatever site they want. This is considered a low severity due to the fact that if Werkzeug is used (which is very common with Flask applications) as the WS ALWAYS ensures that the Location header is absolute - thus making this attack vector mute. It is possible for application writers to modify this default behavior by settir 'autocorrect_location_header=False`.
CVE-2021-23907	An issue was discovered in the Headunit NTG6 in the MBUX Infotainment System on Mercedes-Benz vehicles through 2021. The count in MultiSvGet, GetAttributes, a checked in the HiQnet Protocol, leading to remote code execution.
CVE-2021-23908	An issue was discovered in the Headunit NTG6 in the MBUX Infotainment System on Mercedes-Benz vehicles through 2021. A type confusion issue affects MultiSvSet Protocol, leading to remote code execution.
CVE-2021-29513	TensorFlow is an end-to-end open source platform for machine learning. Calling TF operations with tensors of non-numeric types when the operations expect numeric t pointer dereferences. The conversion from Python array to C++ array(https://github.com/tensorflow/tensorflow/blob/ff70c47a396ef1e3cb73c90513da4f5cb71bebba/tensorflow/python/lib/core/ndarray_tensor.cc#L113-L169) is vulneral The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as th and still in supported range.
CVE-2021-29527	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.QuantizedConv2D`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/00e9a4d67d76703fa1aee33dac582acf317e0e81/tensorflow/core/kernels/quantized_conv_ops.cc#L257-L2 a quantity that is controlled by the caller. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, Tens TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29537	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `QuantizedResizeBilinear` by passing in inval quantization. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/50711818d2e61ccce012591eeb4fdf93a8496726/tensorflow/core/kernels/quantized_resize_bilinear_op.cc that the 2 arguments are always valid scalars and tries to access the numeric value directly. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this co 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29536	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `QuantizedReshape` by passing in invalid thr quantization. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/a324ac84e573fba362a5e53d4e74d5de6729933e/tensorflow/core/kernels/quantized_reshape_op.cc#L38- 2 arguments are always valid scalars and tries to access the numeric value directly. However, if any of these tensors is empty, then `.flat<T>()` is an empty buffer and a at position 0 results in overflow. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2. 2.1.4, as these are also affected and still in supported range.
CVE-2021-29535	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `QuantizedMul` by passing in invalid threshol This is because the implementation(https://github.com/tensorflow/tensorflow/blob/87cf4d3ea9949051e50ca3f071fc909538a51cd0/tensorflow/core/kernels/quantized_m assumes that the 4 arguments are always valid scalars and tries to access the numeric value directly. However, if any of these tensors is empty, then `.flat<T>()` is an e accessing the element at position 0 results in overflow. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlo 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-29534	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.SparseConcat`. Th implementation(https://github.com/tensorflow/tensorflow/blob/b432a38fe0e1b4b904a6c222cbce794c39703e87/tensorflow/core/kernels/sparse_concat_op.cc#L76) take in `shapes[0]` as dimensions for the output shape. The `TensorShape` constructor(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/tensor_shape.cc#L183-L188) us operation which triggers when `InitDims`(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/ten L296) returns a non-OK status. This is a legacy implementation of the constructor and operations should use `BuildTensorShapeBase` or `AddDimWithStatus` to preve the presence of overflows. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 a as these are also affected and still in supported range.
CVE-2021-29533	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK` failure by passing an empty image t `tf.raw_ops.DrawBoundingBoxes`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/ea34a18dc3f5c8d80a40ccca1404f343b5d55f91/tensorflow/core/kernels/image/draw_bounding_box_op.c `CHECK_*` assertions instead of `OP_REQUIRES` to validate user controlled inputs. Whereas `OP_REQUIRES` allows returning an error condition back to the user, t result in a crash if the condition is false, similar to `assert`. In this case, `height` is 0 from the `images` input. This results in `max_box_row_clamp` being negative and t falsified, followed by aborting program execution. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29532	TensorFlow is an end-to-end open source platform for machine learning. An attacker can force accesses outside the bounds of heap allocated arrays by passing in inv `tf.raw_ops.RaggedCross`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/efea03b38fb8d3b81762237dc85e579cc5fc6e87/tensorflow/core/kernels/ragged_cross_op.cc#L456-L487) user supplied arguments. Each of the above branches call a helper function after accessing array elements via a `*_list[next_*]` pattern, followed by incrementing the `n as there is no validation that the `next_*` values are in the valid range for the corresponding `*_list` arrays, this results in heap OOB reads. The fix will be included in Te also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29531	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a `CHECK` fail in PNG encoding by providing an empty input tensor as because the implementation(https://github.com/tensorflow/tensorflow/blob/e312e0791ce486a80c9d23110841525c6f7c3289/tensorflow/core/kernels/image/encode_png validates that the total number of pixels in the image does not overflow. Thus, an attacker can send an empty matrix for encoding. However, if the tensor is empty, then `nullptr`. Hence, when calling `png::WriteImageToBuffer`(https://github.com/tensorflow/tensorflow/blob/e312e0791ce486a80c9d23110841525c6f7c3289/tensorflow/core/kernels/image/encode_png_ first argument (i.e., `image.flat<T>().data()`) is `NULL`. This then triggers the `CHECK_NOTNULL` in the first line of `png::WriteImageToBuffer`(https://github.com/tensorflow/tensorflow/blob/e312e0791ce486a80c9d23110841525c6f7c3289/tensorflow/core/lib/png/png_io.cc#L345-L34 this results in `abort` being called after printing the stacktrace. Effectively, this allows an attacker to mount a denial of service attack. The fix will be included in TensorFl cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29530	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a null pointer dereference by providing an invalid `permutation` to `tf.raw_ops.SparseMatrixSparseCholesky`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/080f1d9e257589f78b3ffb75debf584168aa6062/tensorflow/core/kernels/sparse/sparse_cholesky_op.cc#L validate the input arguments. Although `ValidateInputs` is called and there are checks in the body of this function, the code proceeds to the next line in `ValidateInputs` `OP_REQUIRES`(https://github.com/tensorflow/tensorflow/blob/080f1d9e257589f78b3ffb75debf584168aa6062/tensorflow/core/framework/op_requires.h#L41-L48) is a the current function. Thus, the first validation condition that fails in `ValidateInputs` will cause an early return from that function. However, the caller will continue execut The fix is to either explicitly check `context->status()` or to convert `ValidateInputs` to return a `Status`. The fix will be included in TensorFlow 2.5.0. We will also cherry TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29529	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a heap buffer overflow in `tf.raw_ops.QuantizedResizeBilinear` by mar so that float rounding results in off-by-one error in accessing image elements. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/44b7f486c0143f68b56c34e2d01e146ee445134a/tensorflow/core/kernels/quantized_resize_bilinear_op.cc two integers (representing the upper and lower bounds for interpolation) by ceiling and flooring a floating point value. For some values of `in`, `interpolation->upper[i]` m `interpolation->lower[i]`. This is an issue if `interpolation->upper[i]` is capped at `in_size-1` as it means that `interpolation->lower[i]` points outside of the image. Then, in code(https://github.com/tensorflow/tensorflow/blob/44b7f486c0143f68b56c34e2d01e146ee445134a/tensorflow/core/kernels/quantized_resize_bilinear_op.cc#L245-L26 heap buffer overflow. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and Te these are also affected and still in supported range.
CVE-2021-29528	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.QuantizedMul`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/55900e961ed4a23b438392024912154a2c2f5e85/tensorflow/core/kernels/quantized_mul_op.cc#L188-L19 quantity that is controlled by the caller. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, Tensor TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29538	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a division by zero to occur in `Conv2DBackpropFilter`. This is because implementation(https://github.com/tensorflow/tensorflow/blob/1b0296c3b8dd9bd948f924aa8cd62f87dbb7c3da/tensorflow/core/kernels/conv_grad_filter_ops.cc#L513-L based on user provided data (i.e., the shape of the tensors given as arguments). If all shapes are empty then `work_unit_size` is 0. Since there is no check for this case results in a runtime exception, with potential to be abused for a denial of service. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on Te TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29512	TensorFlow is an end-to-end open source platform for machine learning. If the `splits` argument of `RaggedBincount` does not specify a valid `SparseTensor`(https://www.tensorflow.org/api_docs/python/tf/sparse/SparseTensor), then an attacker can trigger a heap buffer overflow. This will cause a read from o the `splits` tensor buffer in the implementation of the `RaggedBincount` op(https://github.com/tensorflow/tensorflow/blob/8b677d79167799f71c42fd3fa074476e0295413a/tensorflow/core/kernels/bincount_op.cc#L430-L433). Before the `for` l to 0. The user controls the `splits` array, making it contain only one element, 0. Thus, the code in the `while` loop would increment `batch_idx` and then try to read `split of bounds. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3, as these are also affected.
CVE-2021-29514	TensorFlow is an end-to-end open source platform for machine learning. If the `splits` argument of `RaggedBincount` does not specify a valid `SparseTensor`(https://www.tensorflow.org/api_docs/python/tf/sparse/SparseTensor), then an attacker can trigger a heap buffer overflow. This will cause a read from o the `splits` tensor buffer in the implementation of the `RaggedBincount` op(https://github.com/tensorflow/tensorflow/blob/8b677d79167799f71c42fd3fa074476e0295413a/tensorflow/core/kernels/bincount_op.cc#L430-L446). Before the `for` l to 0. The attacker sets `splits(0)` to be 7, hence the `while` loop does not execute and `batch_idx` remains 0. This then results in writing to `out(-1, bin)`, which is before buffer for the output tensor. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3, as these are a

CVE Number	Description
CVE-2021-29554	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in `tf.raw_ops.DenseCountS because the implementation(https://github.com/tensorflow/tensorflow/blob/efff014f3b2d8ef6141da30c806faf141297eca1/tensorflow/core/kernels/count_ops.cc#L123-L1 value from user data but does not check that the result is 0 before doing the division. Since `data` is given by the `values` argument, `num_batch_elements` is 0. The fi TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, and TensorFlow 2.3.3, as these are also affected.
CVE-2021-29526	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.Conv2D`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/988087bd83f144af14087fe4fecee2d250d93737/tensorflow/core/kernels/conv_ops.cc#L261-L263) does a that is controlled by the caller. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2 2.1.4, as these are also affected and still in supported range.
CVE-2021-29525	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.Conv2DBackpropInput`. This is because implementation(https://github.com/tensorflow/tensorflow/blob/b40060c9f697b044e3107917c797ba052f4506ab/tensorflow/core/kernels/conv_grad_input_ops.h#L625-L6 a quantity that is controlled by the caller. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, Tens TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29524	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a division by 0 in `tf.raw_ops.Conv2DBackpropFilter`. This is because implementation(https://github.com/tensorflow/tensorflow/blob/496c2630e51c1a478f095b084329acedb253db6b/tensorflow/core/kernels/conv_grad_shape_utils.cc#L130 operation where the divisor is controlled by the caller. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29523	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.AddManySparseT because the implementation(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/kernels/sparse_tensors_m the values specified in `sparse_shape` as dimensions for the output shape. The `TensorShape` constructor(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/tensor_shape.cc#L183-L188) us operation which triggers when `InitDims`(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/tens L296) returns a non-OK status. This is a legacy implementation of the constructor and operations should use `BuildTensorShapeBase` or `AddDimWithStatus` to preve the presence of overflows. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 a as these are also affected and still in supported range.
CVE-2021-29522	TensorFlow is an end-to-end open source platform for machine learning. The `tf.raw_ops.Conv3DBackprop*` operations fail to validate that the input tensors are not em result in a division by 0. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/a91bb59769f19146d5a0c20060244378e878f140/tensorflow/core/kernels/conv_grad_ops_3d.cc#L430-L45 the divisor used in computing the shard size is not zero. Thus, if attacker controls the input sizes, they can trigger a denial of service via a division by zero error. The fix TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and
CVE-2021-29521	TensorFlow is an end-to-end open source platform for machine learning. Specifying a negative dense shape in `tf.raw_ops.SparseCountSparseOutput` results in a seg thrown out from the standard library as `std::vector` invariants are broken. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/8f7b60ee8c0206a2c99802e3a4d1bb55d2bc0624/tensorflow/core/kernels/count_ops.cc#L199-L213) assu the dense shape is always positive and uses it to initialize a `BatchedMap<T>` (i.e., `std::vector<absl::flat_hash_map<int64,T>>`(https://github.com/tensorflow/tensorflow/blob/8f7b60ee8c0206a2c99802e3a4d1bb55d2bc0624/tensorflow/core/kernels/co structure. If the `shape` tensor has more than one element, `num_batches` is the first value in `shape`. Ensuring that the `dense_shape` argument is a valid tensor sha are non-negative) solves this issue. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3.
CVE-2021-29520	TensorFlow is an end-to-end open source platform for machine learning. Missing validation between arguments to `tf.raw_ops.Conv3DBackprop*` operations can resul overflows. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/4814fafb0ca6b5ab58a09411523b2193fed23fed/tensorflow/core/kernels/conv_grad_shape_utils.cc#L94-L `input`, `filter_sizes` and `out_backprop` tensors have the same shape, as they are accessed in parallel. The fix will be included in TensorFlow 2.5.0. We will also cherr TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29519	TensorFlow is an end-to-end open source platform for machine learning. The API of `tf.raw_ops.SparseCross` allows combinations which would result in a `CHECK`-fa service. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/3d782b7d47b1bf2ed32bd4a246d6d6cadc4c903d/tensorflow/core/kernels/sparse_cross_op.cc#L114-L116 a tensor of type `tstring` which in fact contains integral elements. Fixing the type confusion by preventing mixing `DT_STRING` and `DT_INT64` types solves this issue. in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected ar range.
CVE-2021-29518	TensorFlow is an end-to-end open source platform for machine learning. In eager mode (default in TF 2.0 and later), session operations are invalid. However, users co associated with them and trigger a null pointer dereference. The implementation(https://github.com/tensorflow/tensorflow/blob/eebb96c2830d48597d055d247c0e9aebaea94cd5/tensorflow/core/kernels/session_ops.cc#L104) derefere pointer without checking if it is valid. Thus, in eager mode, `ctx->session_state()` is nullptr and the call of the member function is undefined behavior. The fix will be inclu 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in suppo
CVE-2021-29517	TensorFlow is an end-to-end open source platform for machine learning. A malicious user could trigger a division by 0 in `Conv3D` implementation. The implementation(https://github.com/tensorflow/tensorflow/blob/42033603003965bffac51ae171b51801565e002d/tensorflow/core/kernels/conv_ops_3d.cc#L143-L145) do based on user controlled input. Thus, when `filter` has a 0 as the fifth element, this results in a division by 0. Additionally, if the shape of the two tensors is not valid, an triggered, resulting in a program crash. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, Tensor TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-29516	TensorFlow is an end-to-end open source platform for machine learning. Calling `tf.raw_ops.RaggedTensorToVariant` with arguments specifying an invalid ragged tens pointer dereference. The implementation of `RaggedTensorToVariant` operations(https://github.com/tensorflow/tensorflow/blob/904b3926ed1c6c70380d5313d282d248a776baa1/tensorflow/core/kernels/ragged_tensor_to_variant_op.cc#L3 validate that the ragged tensor argument is non-empty. Since `batched_ragged` contains no elements, `batched_ragged.splits` is a null vector, thus `batched_ragged.s dereferencing `nullptr`. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and ` these are also affected and still in supported range.
CVE-2021-29515	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `MatrixDiag*` operations(https://github.com/tensorflow/tensorflow/blob/4c4f420e68f1cfaf8f4b6e8e3eb857e9e4c3ff33/tensorflow/core/kernels/linalg/matrix_diag_op.cc#L195-L197) do tensor arguments are non-empty. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29600	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `OneHot` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/f61c57bd425878be108ec787f4d96390579fb83e/tensorflow/lite/kernels/one_hot.cc#L68-L72). An attacker can craft a least one of the dimensions of `indices` would be 0. In turn, the `prefix_dim_size` value would become 0. The fix will be included in TensorFlow 2.5.0. We will also cher TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29541	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a dereference of a null pointer in `tf.raw_ops.StringNGrams`. This is be implementation(https://github.com/tensorflow/tensorflow/blob/1cdd4da14282210cc759e468d9781741ac7d01bf/tensorflow/core/kernels/string_ngrams_op.cc#L67-L74) the `data_splits` argument. This would result in `ngrams_data`(https://github.com/tensorflow/tensorflow/blob/1cdd4da14282210cc759e468d9781741ac7d01bf/tensorflow/core/kernels/string_ngrams_op.cc#L106-L11 when the output would be computed to have 0 or negative size. Later writes to the output tensor would then cause a null pointer dereference. The fix will be included in will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range
CVE-2021-29539	TensorFlow is an end-to-end open source platform for machine learning. Calling `tf.raw_ops.ImmutableConst`(https://www.tensorflow.org/api_docs/python/tf/raw_ops/Ir `dtype` of `tf.resource` or `tf.variant` results in a segfault in the implementation as code assumes that the tensor contents are pure scalars. We have patched the issue i 4f663d4b8f0bec1b48da6fa091a7d29609980fa4 and will release TensorFlow 2.5.0 containing the patch. TensorFlow nightly packages after this commit will also have th using `tf.raw_ops.ImmutableConst` in code, you can prevent the segfault by inserting a filter for the `dtype` argument.
CVE-2021-29574	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPool3DGradGrad` exhibits undefined behavior by dere backing attacker-supplied empty tensors. The implementation(https://github.com/tensorflow/tensorflow/blob/72fe792967e7fd25234342068806707bbc116618/tensorflow/core/kernels/pooling_ops_3d.cc#L679-L703) 3 tensor inputs are not empty. If any of them is empty, then accessing the elements in the tensor results in dereferencing a null pointer. The fix will be included in Tensc also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29576	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPool3DGradGrad` is vulnerable to a heap buffer overfl implementation(https://github.com/tensorflow/tensorflow/blob/596c05a159b6fbb9e39ca10b3f7753b7244fa1e9/tensorflow/core/kernels/pooling_ops_3d.cc#L694-L696) c initialization of `Pool3dParameters` completes successfully. Since the constructor(https://github.com/tensorflow/tensorflow/blob/596c05a159b6fbb9e39ca10b3f7753b7244fa1e9/tensorflow/core/kernels/pooling_ops_3d.cc#L48-L88) uses `C validate conditions, the first assertion that fails interrupts the initialization of `params`, making it contain invalid data. In turn, this might cause a heap buffer overflow, de initialized values. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and Tensc are also affected and still in supported range.
CVE-2021-29577	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.AvgPool3DGrad` is vulnerable to a heap buffer overflow. TI implementation(https://github.com/tensorflow/tensorflow/blob/d80ffba9702dc19d1fac74fc4b766b3fa1ee976b/tensorflow/core/kernels/pooling_ops_3d.cc#L376-L450) as `orig_input_shape` and `grad` tensors have similar first and last dimensions but does not check that this assumption is validated. The fix will be included in TensorFlow cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29578	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.FractionalAvgPoolGrad` is vulnerable to a heap buffer over implementation(https://github.com/tensorflow/tensorflow/blob/dcba796a28364d6d7f003f6fe733d82726dda713/tensorflow/core/kernels/fractional_avg_pool_op.cc#L216 the pooling sequence arguments have enough elements as required by the `out_backprop` tensor shape. The fix will be included in TensorFlow 2.5.0. We will also che TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29579	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGrad` is vulnerable to a heap buffer overflow. The implementation(https://github.com/tensorflow/tensorflow/blob/ab1e644b48c82cb71493f4362b4dd38f4577a1cf/tensorflow/core/kernels/maxpooling_op.cc#L194-L203) fa indices used to access elements of input/output arrays are valid. Whereas accesses to `input_backprop_flat` are guarded by `FastBoundsCheck`, the indexing in `out_b result in OOB access. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and T these are also affected and still in supported range.
CVE-2021-29580	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.FractionalMaxPoolGrad` triggers an undefined behavior if c is empty. The code is also vulnerable to a denial of service attack as a `CHECK` condition becomes false and aborts the process. The implementation(https://github.com/tensorflow/tensorflow/blob/169054888d50ce488dfde9ca55d91d6325efbd5b/tensorflow/core/kernels/fractional_max_pool_op.cc#L21 input and output tensors are not empty and are of the same rank. Each of these unchecked assumptions is responsible for the above issues. The fix will be included in will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range
CVE-2021-29581	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.CTCBeamSearchDecoder`, an attacker can trigger den segmentation faults. The implementation(https://github.com/tensorflow/tensorflow/blob/a74768f8e4efbda4def9f16ee7e13cf3922ac5f7/tensorflow/core/kernels/ctc_deco fails to detect cases when the input tensor is empty and proceeds to read data from a null buffer. The fix will be included in TensorFlow 2.5.0. We will also cherrypick th TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29582	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.Dequantize`, an attacker can trigger a read from outsid allocated data. The implementation(https://github.com/tensorflow/tensorflow/blob/26003593aa94b1742f34dc22ce88a1e17776a67d/tensorflow/core/kernels/dequantize_ accesses the `min_range` and `max_range` tensors in parallel but fails to check that they have the same shape. The fix will be included in TensorFlow 2.5.0. We will al commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-29583	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.FusedBatchNorm` is vulnerable to a heap buffer overflow. I the same implementation can trigger undefined behavior by dereferencing null pointers. The implementation(https://github.com/tensorflow/tensorflow/blob/57d86e0db5d1365f19adcce848dfc1bf89fdd4c7/tensorflow/core/kernels/fused_batch_norm_op.cc) fails to `offset`, `mean` and `variance` (the last two only when required) all have the same number of elements as the number of channels of `x`. This results in heap out of bou buffers backing these tensors are indexed past their boundary. If the tensors are empty, the validation mentioned in the above paragraph would also trigger and preven behavior. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2 affected and still in supported range.
CVE-2021-29584	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in caused by an integer overflow tensor shape. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/0908c2f2397c099338b901b067f6495a5b96760b/tensorflow/core/kernels/sparse_split_op.cc#L66-L70) bu without checking that the dimensions would not result in overflow. The `TensorShape` constructor(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/tensor_shape.cc#L183-L188) us operation which triggers when `InitDims`(https://github.com/tensorflow/tensorflow/blob/6f9896890c4c703ae0a0845394086e2e1e523299/tensorflow/core/framework/ten L296) returns a non-OK status. This is a legacy implementation of the constructor and operations should use `BuildTensorShapeBase` or `AddDimWithStatus` to preve the presence of overflows. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 a as these are also affected and still in supported range.
CVE-2021-29585	TensorFlow is an end-to-end open source platform for machine learning. The TFLite computation for size of output after padding, `ComputeOutSize`(https://github.com/tensorflow/tensorflow/blob/0c9692ae7b1671c983569e5d3de5565843d500cf/tensorflow/lite/kernels/padding.h#L43-L55), does not argument is not 0 before doing the division. Users can craft special models such that `ComputeOutSize` is called with `stride` set to 0. The fix will be included in Tensor cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29586	TensorFlow is an end-to-end open source platform for machine learning. Optimized pooling implementations in TFLite fail to check that the stride arguments are not 0 b `ComputePaddingHeightWidth`(https://github.com/tensorflow/tensorflow/blob/3f24ccd932546416ec906a02ddd183b48a1d2c83/tensorflow/lite/kernels/pooling.cc#L90). special models which will have `params->stride_{height,width}` be zero, this will result in a division by zero. The fix will be included in TensorFlow 2.5.0. We will also ch TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29587	TensorFlow is an end-to-end open source platform for machine learning. The `Prepare` step of the `SpaceToDepth` TFLite operator does not check for 0 before division(https://github.com/tensorflow/tensorflow/blob/5f7975d09eac0f10ed8a17dbb6f5964977725adc/tensorflow/lite/kernels/space_to_depth.cc#L63-L67). An attacker that `params->block_size` would be zero. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, Ten TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29588	TensorFlow is an end-to-end open source platform for machine learning. The optimized implementation of the `TransposeConv` TFLite operator is [vulnerable to a divis (https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0179cda284e7e7/tensorflow/lite/kernels/internal/optimized/optimized_ops.h#L5221-L522 a model such that `stride_{h,w}` values are 0. Code calling this function must validate these arguments. The fix will be included in TensorFlow 2.5.0. We will also cherry TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29589	TensorFlow is an end-to-end open source platform for machine learning. The reference implementation of the `GatherNd` TFLite operator is vulnerable to a division by error(https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0179cda284e7e7/tensorflow/lite/kernels/internal/reference/reference_ops.h#L966). A model such that `params` input would be an empty tensor. In turn, `params_shape.Dims(.)` would be zero, in at least one dimension. The fix will be included in TensorF cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29590	TensorFlow is an end-to-end open source platform for machine learning. The implementations of the `Minimum` and `Maximum` TFLite operators can be used to read o of heap allocated objects, if any of the two input tensor arguments are empty. This is because the broadcasting implementation(https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0179cda284e7e7/tensorflow/lite/kernels/internal/reference/maximum_mini indexes in both tensors with the same index but does not validate that the index is within bounds. The fix will be included in TensorFlow 2.5.0. We will also cherrypick th TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29619	TensorFlow is an end-to-end open source platform for machine learning. Passing invalid arguments (e.g., discovered via fuzzing) to `tf.raw_ops.SparseCountSparseOu The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as th and still in supported range.
CVE-2021-29618	TensorFlow is an end-to-end open source platform for machine learning. Passing a complex argument to `tf.transpose` at the same time as passing `conjugate=True` a crash. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4 affected and still in supported range.
CVE-2021-29617	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via `CHECK`-fail in `tf.strings.substr` with invalid arg included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also a supported range.
CVE-2021-29616	TensorFlow is an end-to-end open source platform for machine learning. The implementation of TrySimplify(https://github.com/tensorflow/tensorflow/blob/c22d88d6ff33031aa113e48aa3fc9aa74ed79595/tensorflow/core/grappler/optimizers/arithmetic_optimizer.cc#L undefined behavior due to dereferencing a null pointer in corner cases that result in optimizing a node with no inputs. The fix will be included in TensorFlow 2.5.0. We w commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29615	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `ParseAttrValue`(https://github.com/tensorflow/tensorflow/blob/c22d88d6ff33031aa113e48aa3fc9aa74ed79595/tensorflow/core/framework/attr_value_util.cc#L397-L45 stack overflow due to recursion by giving in a specially crafted input. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4 TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29593	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `BatchToSpaceNd` TFLite operator is vulnerable to a division by ze error(https://github.com/tensorflow/tensorflow/blob/b5ed552fe55895aee8bd8b191f744a069957d18d/tensorflow/lite/kernels/batch_to_space_nd.cc#L81-L82). An attacke such that one dimension of the `block` input is 0. Hence, the corresponding value in `block_shape` is 0. The fix will be included in TensorFlow 2.5.0. We will also cherry TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-29594	TensorFlow is an end-to-end open source platform for machine learning. TFLite's convolution code(https://github.com/tensorflow/tensorflow/blob/09c73bca7d648e961dd05898292d91a8322a9d45/tensorflow/lite/kernels/conv.cc) has multiple division where the div user and not checked to be non-zero. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorF TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29595	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `DepthToSpace` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0179cda284e7e7/tensorflow/lite/kernels/depth_to_space.cc#L63-L69). An attacker c that `params->block_size` is 0. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2 2.1.4, as these are also affected and still in supported range.
CVE-2021-29596	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `EmbeddingLookup` TFLite operator is vulnerable to a division by z error(https://github.com/tensorflow/tensorflow/blob/e4b29809543b250bc9b19678ec4776299dd569ba/tensorflow/lite/kernels/embedding_lookup.cc#L73-L74). An attack such that the first dimension of the `value` input is 0. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29597	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `SpaceToBatchNd` TFLite operator is [vulnerable to a division by ze (https://github.com/tensorflow/tensorflow/blob/412c7d9bb8f8a762c5b266c9e73bfa165f29aac8/tensorflow/lite/kernels/space_to_batch_nd.cc#L82-L83). An attacker can one dimension of the `block` input is 0. Hence, the corresponding value in `block_shape` is 0. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this c 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29598	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `SVDF` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/7f283ff806b2031f407db64c4d3edcda8fb9f9f5/tensorflow/lite/kernels/svdf.cc#L99-L102). An attacker can craft a mod >rank` would be 0. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and Tens are also affected and still in supported range.
CVE-2021-29604	TensorFlow is an end-to-end open source platform for machine learning. The TFLite implementation of hashtable lookup is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/1a8e885b864c818198a5b2c0cbbeca5a1e833bc8/tensorflow/lite/kernels/hashtable_lookup.cc#L114-L115) An attack such that `values`'s first dimension would be 0. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3 TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29603	TensorFlow is an end-to-end open source platform for machine learning. A specially crafted TFLite model could trigger an OOB write on heap in the TFLite implementa `ArgMin`/`ArgMax`(https://github.com/tensorflow/tensorflow/blob/102b211d892f3abc14f845a72047809b39cc65ab/tensorflow/lite/kernels/arg_min_max.cc#L52-L59). If ` value between 0 and `NumDimensions(input)`, then the condition in the `if` is never true, so code writes past the last valid element of `output_dims->data`. The fix will b TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and
CVE-2021-29602	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `DepthwiseConv` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/1a8e885b864c818198a5b2c0cbbeca5a1e833bc8/tensorflow/lite/kernels/depthwise_conv.cc#L287-L288). An attacke such that `input`'s fourth dimension would be 0. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3 TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29540	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow to occur in `Conv2DBackpropFilter`. This is beca implementation(https://github.com/tensorflow/tensorflow/blob/1b0296c3b8dd9bd948f924aa8cd62f87dbb7c3da/tensorflow/core/kernels/conv_grad_filter_ops.cc#L495-L of the filter tensor but does not validate that it matches the number of elements in `filter_sizes`. Later, when reading/writing to this buffer, code uses the value computed number of elements in the tensor. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29575	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.ReverseSequence` allows for stack overflow and/or `CHEC service. The implementation(https://github.com/tensorflow/tensorflow/blob/5b3b071975e01f0d250c928b2a8f901cd53b90a7/tensorflow/core/kernels/reverse_sequence_ to validate that `seq_dim` and `batch_dim` arguments are valid. Negative values for `seq_dim` can result in stack overflow or `CHECK`-failure, depending on the versio implement the operation. Similar behavior can be exhibited by invalid values of `batch_dim`. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this co 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29573	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` is vulnerable to a division by 0. implementation(https://github.com/tensorflow/tensorflow/blob/279bab6efa22752a2827621b7edb56a730233bd8/tensorflow/core/kernels/maxpooling_op.cc#L1033-L103 the batch dimension of the tensor is non-zero, before dividing by this quantity. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on Tens TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29556	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in `tf.raw_ops.Reverse`. Thi implementation(https://github.com/tensorflow/tensorflow/blob/36229ea9e9451dac14a8b1f4711c435a1d84a594/tensorflow/core/kernels/reverse_op.cc#L75-L76) perfor the first dimension of the tensor argument. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, Ter TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29599	TensorFlow is an end-to-end open source platform for machine learning. The implementation of the `Split` TFLite operator is vulnerable to a division by zero error(https://github.com/tensorflow/tensorflow/blob/e2752089ef7ce9bcf3db0ec618ebd23ea119d0c7/tensorflow/lite/kernels/split.cc#L63-L65). An attacker can craft a mo `num_splits` would be 0. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 an these are also affected and still in supported range.
CVE-2021-29542	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow by passing crafted inputs to `tf.raw_ops.StringN because the implementation(https://github.com/tensorflow/tensorflow/blob/1cdd4da14282210cc759e468d9781741ac7d01bf/tensorflow/core/kernels/string_ngrams_op. consider corner cases where input would be split in such a way that the generated tokens should only contain padding elements. If input is such that `num_tokens` is 0, `data_start_index=0` (when left padding is present), the marked line would result in reading `data[-1]`. The fix will be included in TensorFlow 2.5.0. We will also cherryp TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-29543	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.CTCGreedyDecod implementation(https://github.com/tensorflow/tensorflow/blob/1615440b17b364b875eb06f43d087381f1460a65/tensorflow/core/kernels/ctc_decoder_ops.cc#L37-L50) h inserted to validate some invariants. When this condition is false, the program aborts, instead of returning a valid error to the user. This abnormal termination can be we service attacks. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorI also affected and still in supported range.
CVE-2021-29544	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in `tf.raw_ops.QuantizeAndDequ because the implementation does not validate the rank of the `input_*` tensors. In turn, this results in the tensors being passes as they are to `QuantizeAndDequantizePerChannelGradientImpl`. However, the `vec<T>` method, requires the rank to 1 and triggers a `CHECK` failure otherwise. The fix will be inclu 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 as this is the only other affected version.
CVE-2021-29545	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a denial of service via a `CHECK`-fail in converting sparse tensors to C This is because the implementation(https://github.com/tensorflow/tensorflow/blob/800346f2c03a27e182dd4fba48295f65e7790739/tensorflow/core/kernels/sparse/kerne double redirection to access an element of an array allocated on the heap. If the value at `indices(i, 0)` is such that `indices(i, 0) + 1` is outside the bounds of `csr_row_ writing outside of bounds of heap allocated data. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29546	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger an integer division by zero undefined behavior in `tf.raw_ops.Quantize because the implementation of the Eigen kernel(https://github.com/tensorflow/tensorflow/blob/61bca8bd5ba8a68b2d97435ddfafcdf2b85672cd/tensorflow/core/kernels/quantization_utils.h#L812-L849) does a di elements of the smaller input (based on shape) without checking that this is not zero. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit o TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29547	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a segfault and denial of service via accessing data outside of bounds ir `tf.raw_ops.QuantizedBatchNormWithGlobalNormalization`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/55a97caa9e99c7f37a0bbbeb414dc55553d3ae7f/tensorflow/core/kernels/quantized_batch_norm_op.cc#L inputs are not empty. If any of these inputs is empty, `.flat<T>()` is an empty buffer, so accessing the element at index 0 is accessing data outside of bounds. The fix wi TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and
CVE-2021-29548	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a runtime division by zero error and denial of service in `tf.raw_ops.QuantizedBatchNormWithGlobalNormalization`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/55a97caa9e99c7f37a0bbbeb414dc55553d3ae7f/tensorflow/core/kernels/quantized_batch_norm_op.cc) d constraints specified in the op's contract(https://www.tensorflow.org/api_docs/python/tf/raw_ops/QuantizedBatchNormWithGlobalNormalization). The fix will be included We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported ra
CVE-2021-29549	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a runtime division by zero error and denial of service in `tf.raw_ops.QuantizedBatchNormWithGlobalNormalization`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/6f26b3f3418201479c264f2a02000880d8df151c/tensorflow/core/kernels/quantized_add_op.cc#L289-L295 operation without validating that the divisor is not zero. Since `vector_num_elements` is determined based on input shapes(https://github.com/tensorflow/tensorflow/blob/6f26b3f3418201479c264f2a02000880d8df151c/tensorflow/core/kernels/quantized_add_op.cc#L522-L544), a user where this quantity is 0. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and these are also affected and still in supported range.
CVE-2021-29550	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a runtime division by zero error and denial of service in `tf.raw_ops.Fra because the implementation(https://github.com/tensorflow/tensorflow/blob/acc8ee69f5f46f92a3f1f11230f49c6ac266f10c/tensorflow/core/kernels/fractional_avg_pool_op computes a divisor quantity by dividing two user controlled values. The user controls the values of `input_size[i]` and `pooling_ratio_[i]` (via the `value.shape()` and `poo If the value in `input_size[i]` is smaller than the `pooling_ratio_[i]`, then the floor operation results in `output_size[i]` being 0. The `DCHECK_GT` line is a no-op outside released versions of TF this does not trigger. Later, these computed values are used as arguments(https://github.com/tensorflow/tensorflow/blob/acc8ee69f5f46f92a3f1f11230f49c6ac266f10c/tensorflow/core/kernels/fractional_avg_pool_op.cc#L96-L99) to `GeneratePoolingSequence`(https://github.com/tensorflow/tensorflow/blob/acc8ee69f5f46f92a3f1f11230f49c6ac266f10c/tensorflow/core/kernels/fractional_pool_comm There, the first computation is a division in a modulo operation. Since `output_length` can be 0, this results in runtime crashing. The fix will be included in TensorFlow 2 cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29551	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `MatrixTriangularSolve`(https://github.com/tensorflow/tensorflow/blob/8cae746d8449c7dda5298327353d68613f16e798/tensorflow/core/kernels/linalg/matrix_triangular_ L240) fails to terminate kernel execution if one validation condition fails. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29552	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by controlling the values of `num_segments` tensor `UnsortedSegmentJoin`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/a2a607db15c7cd01d754d37e5448d72a13491bdb/tensorflow/core/kernels/unsorted_segment_join_op.cc# the `num_segments` tensor is a valid scalar. Since the tensor is empty the `CHECK` involved in `.scalar<T>()()` that checks that the number of elements is exactly 1 wi this would result in process termination. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, Tenso TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29553	TensorFlow is an end-to-end open source platform for machine learning. An attacker can read data outside of bounds of heap allocated buffer in `tf.raw_ops.QuantizeA is because the implementation(https://github.com/tensorflow/tensorflow/blob/11ff7f80667e6490d7b5174aa6bf5e01886e770f/tensorflow/core/kernels/quantize_and_deq does not validate the value of user supplied `axis` attribute before using it to index in the array backing the `input` argument. The fix will be included in TensorFlow 2.5.(cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29555	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in `tf.raw_ops.FusedBatchN the implementation(https://github.com/tensorflow/tensorflow/blob/828f346274841fa7505f7020e88ca36c22e557ab/tensorflow/core/kernels/fused_batch_norm_op.cc#L2 division based on the last dimension of the `x` tensor. Since this is controlled by the user, an attacker can trigger a denial of service. The fix will be included in TensorFl cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-29557	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in `tf.raw_ops.SparseMatMu occurs deep in Eigen code because the `b` tensor is empty. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, Tens TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29559	TensorFlow is an end-to-end open source platform for machine learning. An attacker can access data outside of bounds of heap allocated array in `tf.raw_ops.Unicode because the implementation(https://github.com/tensorflow/tensorflow/blob/472c1f12ad9063405737679d4f6bd43094e1d36d/tensorflow/core/kernels/unicode_ops.cc) as `input_value`/`input_splits` pair specify a valid sparse tensor. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, Ten TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29560	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `tf.raw_ops.RaggedTensorToTensor`. This is implementation(https://github.com/tensorflow/tensorflow/blob/d94227d43aa125ad8b54115c03cece54f6a1977b/tensorflow/core/kernels/ragged_tensor_to_tensor_op.cc same index to access two arrays in parallel. Since the user controls the shape of the input arguments, an attacker could trigger a heap OOB access when `parent_outp than `row_split`. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and Tensor are also affected and still in supported range.
CVE-2021-29561	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by exploiting a `CHECK`-failure coming from `tf.raw_ops.LoadAndRemapMatrix`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/d94227d43aa125ad8b54115c03cece54f6a1977b/tensorflow/core/kernels/ragged_tensor_to_tensor_op.cc that the `ckpt_path` is always a valid scalar. However, an attacker can send any other tensor as the first argument of `LoadAndRemapMatrix`. This would cause the rar `scalar<T>()()` to trigger and terminate the process. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29562	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by exploiting a `CHECK`-failure coming from the imp `tf.raw_ops.IRFFT`. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and Ten are also affected and still in supported range.
CVE-2021-29563	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service by exploiting a `CHECK`-failure coming from the imp `tf.raw_ops.RFFT`. Eigen code operating on an empty matrix can trigger on an assertion and will cause program termination. The fix will be included in TensorFlow 2.5. cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29564	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a null pointer dereference in the implementation of `tf.raw_ops.EditDist the implementation(https://github.com/tensorflow/tensorflow/blob/79865b542f9ffdc9caeb255631f7c56f1d4b6517/tensorflow/core/kernels/edit_distance_op.cc#L103-L15 validation of the input parameters. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29565	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger a null pointer dereference in the implementation of `tf.raw_ops.SparseF because of missing validation(https://github.com/tensorflow/tensorflow/blob/fdc82089d206e281c628a93771336bf87863d5e8/tensorflow/core/kernels/sparse_fill_empty_ L231) that was covered under a `TODO`. If the `dense_shape` tensor is empty, then `dense_shape_t.vec<>()` would cause a null pointer dereference in the implement will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are in supported range.
CVE-2021-29566	TensorFlow is an end-to-end open source platform for machine learning. An attacker can write outside the bounds of heap allocated arrays by passing invalid argumen `tf.raw_ops.Dilation2DBackpropInput`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/afd954e65f15aea4d438d0a219136fc4a63a573d/tensorflow/core/kernels/dilation_ops.cc#L321-L322) does writing to the output array. The values for `h_out` and `w_out` are guaranteed to be in range for `out_backprop` (as they are loop indices bounded by the size of the arr no similar guarantees relating `h_in_max`/`w_in_max` and `in_backprop`. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlo 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29567	TensorFlow is an end-to-end open source platform for machine learning. Due to lack of validation in `tf.raw_ops.SparseDenseCwiseMul`, an attacker can trigger denial `CHECK`-fails or accesses to outside the bounds of heap allocated data. Since the implementation(https://github.com/tensorflow/tensorflow/blob/38178a2f7a681a7835bb0912702a134bfe3b4d84/tensorflow/core/kernels/sparse_dense_binary_op_share validates the rank of the input arguments but no constraints between dimensions(https://www.tensorflow.org/api_docs/python/tf/raw_ops/SparseDenseCwiseMul), an at to trigger internal `CHECK` assertions (and cause program termination, denial of service) or to write to memory outside of bounds of heap allocated tensor buffers. The TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and
CVE-2021-29568	TensorFlow is an end-to-end open source platform for machine learning. An attacker can trigger undefined behavior by binding to null pointer in `tf.raw_ops.Parameteri This is because the implementation(https://github.com/tensorflow/tensorflow/blob/3f6fe4dfef6f57e768260b48166c27d148f3015f/tensorflow/core/kernels/parameterized_truncated_normal_c validate input arguments before accessing the first element of `shape`. If `shape` argument is empty, then `shape_tensor.flat<T>()` is an empty array. The fix will be inc 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in suppo
CVE-2021-29569	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of bou data if attacker supplies specially crafted inputs. The implementation(https://github.com/tensorflow/tensorflow/blob/ac328eaa3870491ababc147822cd04e91a790643/tensorflow/core/kernels/requantization_range_op.cc#L4 the `input_min` and `input_max` tensors have at least one element, as it accesses the first element in two arrays. If the tensors are empty, `.flat<T>()` is an empty objec array. Hence, accesing even the 0th element is a read outside the bounds. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorF 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29570	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of bou data if attacker supplies specially crafted inputs. The implementation(https://github.com/tensorflow/tensorflow/blob/ef0c008ee84bad91ec6725ddc42091e19a30cf0e/tensorflow/core/kernels/maxpooling_op.cc#L1016-L1017 to index in two different arrays but there is no guarantee that the sizes are identical. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE Number	Description
CVE-2021-29572	TensorFlow is an end-to-end open source platform for machine learning. The implementation of `tf.raw_ops.SdcaOptimizer` triggers undefined behavior due to derefere The implementation(https://github.com/tensorflow/tensorflow/blob/60a45c8b6192a4699f2e2709a2645a751d435cc3/tensorflow/core/kernels/sdca_internal.cc) does not supplied arguments satisfy all constraints expected by the op(https://www.tensorflow.org/api_docs/python/tf/raw_ops/SdcaOptimizer). The fix will be included in Tensor cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2021-29558	TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a heap buffer overflow in `tf.raw_ops.SparseSplit`. This is because the implementation(https://github.com/tensorflow/tensorflow/blob/699bff5d961f0abfde8fa3f876e6d241681fbef8/tensorflow/core/util/sparse/sparse_tensor.h#L528-L530) acc element based on a user controlled offset. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, Ter TensorFlow 2.1.4, as these are also affected and still in supported range.
CVE-2020-4811	IBM Cloud Pak for Security (CP4S) 1.4.0.0, 1.5.0.0, 1.5.0.1, 1.6.0.0, and 1.6.0.1 could allow a privileged user to inject inject malicious data using a specially crafted HT improper input validation.
CVE-2021-23906	An issue was discovered in the Headunit NTG6 in the MBUX Infotainment System on Mercedes-Benz vehicles through 2021. A Message Length is not checked in the H leading to remote code execution.