

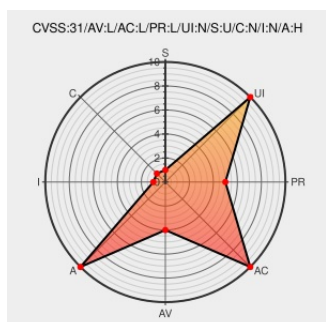


CVE-2022-29212

Published on: Not Yet Published

Last Modified on: 06/03/2022 03:16:00 PM UTC

CVE-2022-29212 - advisory for GHSA-8www-6264-x792

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

Certain versions of [Tensorflow](#) from [Google](#) contain the following vulnerability:

TensorFlow is an open source platform for machine learning. Prior to versions 2.9.0, 2.8.1, 2.7.2, and 2.6.4, certain TFLite models that were created using TFLite model converter would crash when loaded in the TFLite interpreter. The culprit is that during quantization the scale of values could be greater than 1 but code was always assuming sub-unit scaling. Thus, since code was calling `QuantizeMultiplierSmallerThanOneExp`, the `TFLITE\_CHECK\_LT` assertion would trigger and abort the process. Versions 2.9.0, 2.8.1, 2.7.2, and 2.6.4 contain a patch for this issue.

CVE-2022-29212 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version < 2.6.4

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version >= 2.7.0rc0, < 2.7.2

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version >= 2.8.0rc0, < 2.8.1

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version >= 2.9.0rc0, < 2.9.0

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **2.1 - LOW**

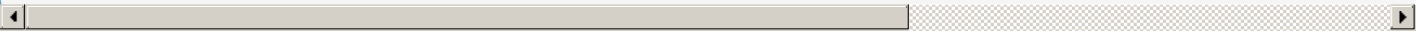
Access Vector	Access Complexity	Authentication
---------------	-------------------	----------------

LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Release TensorFlow 2.8.1 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.8.1
Core dumped when invoking TFLite model converted using latest nightly TFLite converter (2.4.0dev2020929) · Issue #43661 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/issues/43661
Improve to cover scale value greater than one · tensorflow/tensorflow@a989426 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/a989426ee1346693cc015
tensorflow/quantization_util.cc at f3b9bf4c3c0597563b289c0512e98d4ce81f886e · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/f3b9bf4c3c0597563b289c0512e98d4ce81f886e
Release TensorFlow 2.9.0 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.9.0
Release TensorFlow 2.7.2 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.7.2
Release TensorFlow 2.6.4 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.6.4
Core dump when loading TFLite models with quantization · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-8w8p-3p3p-3p3p

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.



There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.7.0	rc0	All	All
Application	Google	Tensorflow	2.7.0	rc1	All	All
Application	Google	Tensorflow	2.8.0	-	All	All
Application	Google	Tensorflow	2.8.0	rc0	All	All
Application	Google	Tensorflow	2.8.0	rc1	All	All
Application	Google	Tensorflow	2.9.0	rc0	All	All

No vendor comments have been submitted for this CVE

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29212 : TensorFlow is an open source platform for machine learning. Prior to versions 2.9.0, 2.8.1, 2.7.2,... twitter.com/i/web/status/1...	2022-05-20 23:17:42
@LinInfoSec	Tensorflow - CVE-2022-29212: github.com/tensorflow/ten...	2022-05-21 06:00:52
/r/netcve	CVE-2022-29212	2022-05-21 00:38:10

Next ID→

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE.report and Source URL Uptime Status status.cve.report