



CVE-2021-29548

Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 05/20/2021 03:17:00 PM UTC

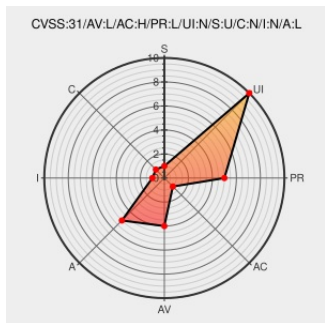
CVE-2021-29548 - advisory for GHSA-p45v-v4pw-77jr

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Tensorflow** from **Google** contain the following vulnerability:

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/55a97caa9e99c7f37a0bbbeb414>) does not validate all constraints specified in the op's contract(https://www.tensorflow.org/api_docs/python/tf/raw_ops/QuantizedBatchNormWithGlob). 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 these are also affected and still in supported range.

CVE-2021-29548 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version < 2.1.4

Affected Vendor/Software: **tensorflow** - **tensorflow** version >= 2.2.0, < 2.2.3

Affected Vendor/Software: **tensorflow** - **tensorflow** version >= 2.3.0, < 2.3.3

Affected Vendor/Software: **tensorflow** - **tensorflow** version >= 2.4.0, < 2.4.2

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
Add missing validation in <code>`QuantizedBatchNormWithGlobalNormalization`</code> · tensorflow/tensorflow@d6ed5bc · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/d6ed5bcfe1dcab9e85a4d39931bd1
Division by 0 in <code>`QuantizedBatchNormWithGlobalNormalization`</code> · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-p4

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.

Related QID Numbers

982501 Python (pip) Security Update for tensorflow-gpu (GHSA-p45v-v4pw-77jr)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
cpe:2.3:a:google:tensorflow:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID →

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)