



CVE-2021-29539

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

Last Modified on: 07/27/2021 05:26:00 PM UTC

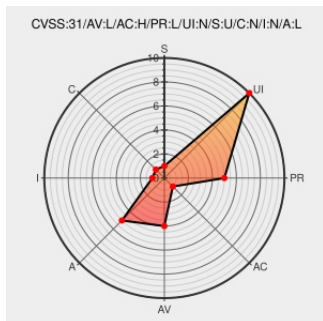
CVE-2021-29539 - advisory for GHSA-g4h2-gqm3-c9wq

[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. Calling

``tf.raw_ops.ImmutableConst`` (https://www.tensorflow.org/api_docs/python/tf/raw_ops/ImmutableConst) with a ``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 in 4f663d4b8f0bec1b48da6fa091a7d29609980fa4 and will release TensorFlow 2.5.0 containing the patch. TensorFlow nightly packages after this commit will also have the issue resolved. If using ``tf.raw_ops.ImmutableConst`` in code, you can prevent the segfault by inserting a filter for the ``dtype`` argument.

CVE-2021-29539 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

cpe:2.3:a:google:tensorflow:*.*.*.*.*.*.*.*
cpe:2.3:a:google:tensorflow:*.*.*.*.*.*.*.*
cpe:2.3:a:google:tensorflow:*.*.*.*.*.*.*.*
cpe:2.3:a:google:tensorflow:*.*.*.*.*.*.*.*
cpe:2.3:a:google:tensorflow:*.*.*.*.*.*.*.*
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 →