

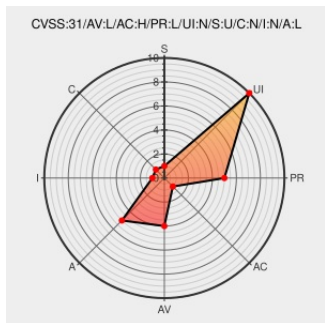


CVE-2021-29538

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

Last Modified on: 07/27/2021 05:30:00 PM UTC

CVE-2021-29538 - advisory for GHSA-j8qc-5fqr-52fp

[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 division by zero to occur in `Conv2DBackpropFilter`. This is because the

implementation(<https://github.com/tensorflow/tensorflow/blob/1b0296c3b8dd9bd948f924aa8cdL522>) computes a divisor 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 before division, this 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 cherry-pick 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-2021-29538 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→		