

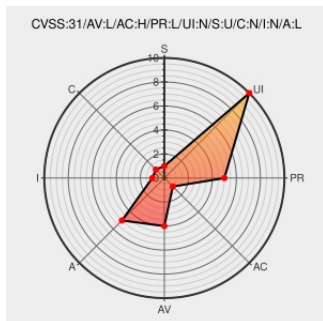


CVE-2021-29517

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

Last Modified on: 05/20/2021 04:27:00 PM UTC

CVE-2021-29517 - advisory for GHSA-772p-x54p-hjrv

[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. A malicious user could trigger a division by 0 in `Conv3D` implementation. The

implementation(<https://github.com/tensorflow/tensorflow/blob/42033603003965bffa51ae171b5L145>) does a modulo operation 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 Eigen assertion can be 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, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE-2021-29517 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

Division by zero in `Conv3D` · Advisory · tensorflow/tensorflow · GitHub

github.com

text/html

CONFIRM

github.com/tensorflow/tensorflow/security/advisories/GHSA-772p-x54p-hjrv

Fix 2 issues with `Conv3D` · tensorflow/tensorflow@799f835 · GitHub

github.com

text/html

MISC

github.com/tensorflow/tensorflow/commit/799f835a3dfa00a4d852defa29b15841eea9d64f

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

982529 Python (pip) Security Update for tensorflow-gpu (GHSA-772p-x54p-hjrv)

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)

🐦 @CVEreport

CVE-2021-29517 : TensorFlow is an end-to-end open source platform for machine learning. A malicious user could trig... twitter.com/i/web/status/1...

2021-05-14 20:09:49

👤 /r/netcve

CVE-2021-29517

2021-05-14 20:41:11

← Previous ID

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, 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](#)