

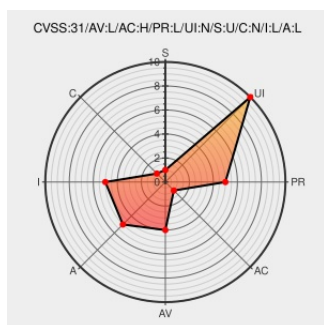


CVE-2021-29611

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

Last Modified on: 05/18/2021 07:17:00 PM UTC

CVE-2021-29611 - advisory for GHSA-9rpc-5v9q-5r7f

[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. Incomplete validation in `SparseReshape` results in a denial of service based on a `CHECK`-failure. The

implementation(<https://github.com/tensorflow/tensorflow/blob/e87b51ce05c3eb172065a6ea5f4>) has no validation that the input arguments specify a valid sparse tensor. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2 and TensorFlow 2.3.3, as these are the only affected versions.

CVE-2021-29611 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [tensorflow](#) - tensorflow version < 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	Integrity	Availability

Impact	Impact	Impact				
NONE	NONE	PARTIAL				
CVE References						
Description	Tags	Link				
Fix heap-buffer-overflow issue with <code>`tf.raw_ops.SparseReshape`</code> . · tensorflow/tensorflow@1d04d7d · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/1d04d7d93f4ed3854abf75d6b712d72c3f70d6b6				
Incomplete validation in <code>`SparseReshape`</code> · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-9rpc-5v9q-5r7f				
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						
982444 Python (pip) Security Update for tensorflow-gpu (GHSA-9rpc-5v9q-5r7f)						
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 →			