



CVE-2021-41198

Published on: 11/05/2021 12:00:00 AM UTC

Last Modified on: 11/17/2021 09:38:18 PM UTC

CVE-2021-41198 - advisory for GHSA-2p25-55c9-h58q

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H



Certain versions of [Tensorflow](#) from [Google](#) contain the following vulnerability:

TensorFlow is an open source platform for machine learning. In affected versions if `tf.tile` is called with a large input argument then the TensorFlow process will crash due to a `CHECK`-failure caused by an overflow. The number of elements in the output tensor is too much for the `int64\_t` type and the overflow is detected via a `CHECK`

statement. This aborts the process. The fix will be included in TensorFlow 2.7.0. We will also cherry-pick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.

CVE-2021-41198 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version $\geq 2.6.0$, $< 2.6.1$

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version $\geq 2.5.0$, $< 2.5.2$

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version $< 2.4.4$

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

Confidentiality Impact

NONE

Integrity Impact

NONE

Availability Impact

PARTIAL

CVE References

Description

tf.keras.backend.tile crash(aborts) when n is large · Issue #46911 · tensorflow/tensorflow · GitHub

Tags

github.com

text/html

Link

 MISC github.com/tensorflow/tensorflow/issues/46911

Description

Overflow/crash in `tf.tile` when tiling tensor is large · Advisory · tensorflow/tensorflow · GitHub

Tags

github.com

text/html

Link

 CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-2p25-55c9-h58q

Description

Merge pull request #51138 from yongtang:46911-tile · tensorflow/tensorflow@9294094 · GitHub

Tags

github.com

text/html

Link

 MISC github.com/tensorflow/tensorflow/commit/9294094df6fea79271778eb7e7ae1bad8b5ef98f

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

980164 Python (pip) Security Update for tensorflow-gpu (GHSA-2p25-55c9-h58q)

Known Affected Configurations (CPE V2.3)

Type

Application

Vendor

Google

Product

Tensorflow

Version

All

Update

All

Edition

All

Language

All

cpe:2.3:a:google:tensorflow:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source

@CVEreport

Title

CVE-2021-41198 : TensorFlow is an open source platform for machine learning. In affected versions if `tf.tile` is c... twitter.com/i/web/status/1...

Posted (UTC)

2021-11-05 20:05:21

← Previous ID

Next ID →

[site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report