



CVE-2022-35968

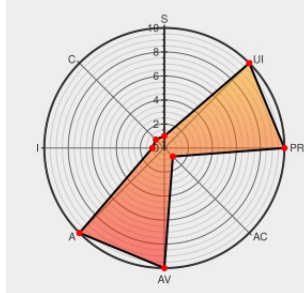
Published on: Not Yet Published

Last Modified on: 09/20/2022 08:06:00 PM UTC

CVE-2022-35968 - advisory for GHSA-2475-53vw-vp25

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

CVSS:31/AV:N/AC:H/PR:N/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. The implementation of `AvgPoolGrad` does not fully validate the input `orig\_input\_shape`. This results in a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 3a6ac52664c6c095aa2b114e742b0aa17fdce78f. The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.

CVE-2022-35968 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [tensorflow](#) - tensorflow version < 2.7.2

Affected Vendor/Software: [tensorflow](#) - tensorflow version >= 2.8.0, < 2.8.1

Affected Vendor/Software: [tensorflow](#) - tensorflow version >= 2.9.0, < 2.9.1

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVE References

Description	Tags	Link
`CHECK` fail in `AvgPoolGrad` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-2475-53vw-vp25

github.com/tensorflow/tensorflow/commit/3a6ac52664c6c095aa2b114e742b0aa17fdce78f

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](#)