



CVE-2022-36003

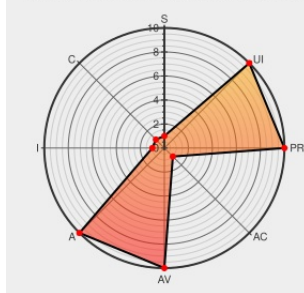
Published on: Not Yet Published

Last Modified on: 09/20/2022 02:42:00 PM UTC

CVE-2022-36003 - advisory for GHSA-cv2p-32v3-vhwq

[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. When `RandomPoissonV2` receives large input shape and rates, it gives a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit

552bfced6ce4809db5f3ca305f60ff80dd40c5a3. 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-2022-36003 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
Fix size check for large input shape and rates. · tensorflow/tensorflow@552bfce ·	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/552bfced6ce4809db5f3ca305f60ff80dd40c5a3

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](#)