



CVE-2022-35989

Published on: Not Yet Published

Last Modified on: 09/20/2022 02:54:00 PM UTC

CVE-2022-35989 - advisory for GHSA-j43h-pgmg-5hjq

[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 `MaxPool` receives a window size input array `ksize` with dimensions greater than its input tensor `input`, the GPU kernel gives a `CHECK` fail that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit

32d7bd3defd134f21a4e344c8dfd40099aaf6b18. 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-2022-35989 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 `MaxPool` · Advisory · tensorflow/tensorflow ·	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-j43h-pgmg-5hjq

There are currently no QIDs associated with this CVE

No vendor comments have been submitted for this CVE

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