

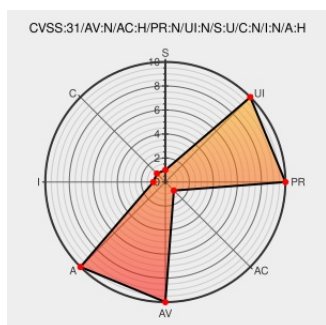


CVE-2022-35986

Published on: Not Yet Published

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

CVE-2022-35986 - advisory for GHSA-wr9v-g9vf-c74v

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

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

TensorFlow is an open source platform for machine learning. If `RaggedBincount` is given an empty input tensor `splits`, it results in a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit

7a4591fd4f065f4fa903593bc39b2f79530a74b8. 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-2022-35986 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 RaggedBincount Segmentation Fault from the Splits arg · tensorflow/tensorflow@7a4591f ·	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/7a4591fd4f065f4fa903593bc39b2f79530a74b8

GitHub

Segfault in `RaggedBincount` · Advisory · tensorflow/tensorflow · GitHub

[github.com](#)[text/html](#)

 **CONFIRM** github.com/tensorflow/tensorflow/security/advisories/GHSA-wr9v-g9vf-c74v

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.10	rc0	All	All
Application	Google	Tensorflow	2.10	rc1	All	All
Application	Google	Tensorflow	2.10	rc2	All	All
Application	Google	Tensorflow	2.10	rc3	All	All

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

cpe:2.3:a:google:tensorflow:2.10:rc0:*.:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.10:rc1:*.:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.10:rc2:*.:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.10:rc3:*.:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2022-35986	2022-09-16 22:38:47

← Previous ID

Next ID →

