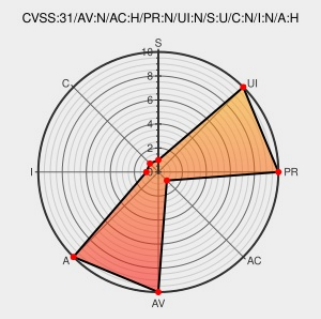
CVE-2022-35969

Published on: Not Yet Published

Last Modified on: 09/20/2022 07:58:00 PM UTC

CVE-2022-35969 - advisory for GHSA-q2c3-jpmc-gfjx

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. The implementation of `Conv2DBackpropInput` requires `input_sizes` to be 4-dimensional. Otherwise, it gives a `CHECK` failure which can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 50156d547b9a1da0144d7babe665cf690305b33c. The fix will be included in TensorFlow 2.10.0. We will also cherrypick 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-2022-35969 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
Add security vulnerability test for raw_ops.Conv2DBackpropInput .	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/50156d547b9a1da0144d7babe665cf690305b33c

tensorflow/tensorflow@50156d5 · GitHub		
`CHECK` fail in `Conv2DBackpropInput` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-q2c3-jpmc-gfjx

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)
@CVEreport	CVE-2022-35969 : TensorFlow is an open source platform for machine learning. The implementation of `Conv2DBackpropI… twitter.com/i/web/status/1…	2022-09-16 20:54:02
/r/netcve	CVE-2022-35969	2022-09-16 21:38:41

← Previous ID

Next ID→

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