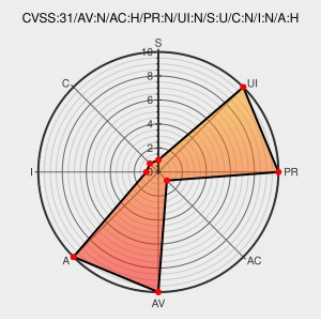
CVE-2022-35981

Published on: Not Yet Published

Last Modified on: 09/20/2022 02:53:00 PM UTC

CVE-2022-35981 - advisory for GHSA-vxv8-r8q2-63xw

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. `FractionalMaxPoolGrad` validates its inputs with `CHECK` failures instead of with returning errors. If it gets incorrectly sized inputs, the `CHECK` failure can be used to trigger a denial of service attack. We have patched the issue in GitHub commit 8741e57d163a079db05a7107a7609af70931def4. 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-2022-35981 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 `FractionalMaxPoolGrad` ·	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-vxv8-r8q2-63xw

Advisory · tensorflow/tensorflow · GitHub		
Fix security vulnerability with FractionalMaxPoolGrad · tensorflow/tensorflow@8741e57 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/8741e57d163a079db05a7107a7609af70931def4

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-2022-35981 : TensorFlow is an open source platform for machine learning. `FractionalMaxPoolGrad` validates its… twitter.com/i/web/status/1…	2022-09-16 21:23:06

← Previous ID

Next ID→

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