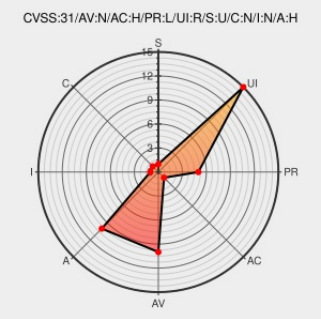
CVE-2022-41910

Published on: Not Yet Published

Last Modified on: 12/08/2022 02:59:00 AM UTC

CVE-2022-41910 - advisory for GHSA-frqp-wp83-qggv

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 function MakeGrapplerFunctionItem takes arguments that determine the sizes of inputs and outputs. If the inputs given are greater than or equal to the sizes of the outputs, an out-of-bounds memory read or a crash is triggered. We have patched the issue in GitHub commit a65411a1d69edfb16b25907ffb8f73556ce36bb7. The fix will be included in TensorFlow 2.11.0. We will also cherrypick this commit on TensorFlow 2.8.4, 2.9.3, and 2.10.1.

CVE-2022-41910 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.10.0, < 2.10.1**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.9.0, < 2.9.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 2.8.4**

CVSS3 Score: 9.1 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	HIGH

CVE References

Description	Tags	Link
Fix OOB write in grappler. · tensorflow/tensorflow@a65411a · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/a65411a1d69edfb16b25907ffb8f73556ce36bb7

Heap overflow in `QuantizeAndDequantizeV2` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-frqp-wp83-qggv
tensorflow/functions.cc at master · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/master/tensorflow/core/grappler/utils/functions.cc#L22

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	2.10.0	-	All	All

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

cpe:2.3:a:google:tensorflow:2.10.0:-:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-41910 : TensorFlow is an open source platform for machine learning. The function MakeGrapplerFunctionItem… twitter.com/i/web/status/1…	2022-12-06 21:22:56
/r/netcve	CVE-2022-41910	2022-12-06 22:42:58

← Previous ID

Next ID→