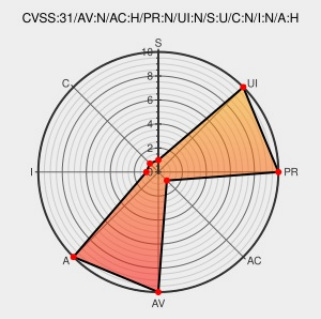
CVE-2022-35973

Published on: Not Yet Published

Last Modified on: 09/20/2022 07:12:00 PM UTC

CVE-2022-35973 - advisory for GHSA-689c-r7h2-fv9v

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 `QuantizedMatMul` is given nonscalar input for: `min_a`, `max_a`, `min_b`, or `max_b` It gives a segfault that can be used to trigger a denial of service attack. We have patched the issue in GitHub commit aca766ac7693bf29ed0df55ad6bfcc78f35e7f48. 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-2022-35973 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 tf.raw_ops. QuantizedMatMul vulnerability from non scalar min/max… ·	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/aca766ac7693bf29ed0df55ad6bfcc78f35e7f48

tensorflow/tensorflow@aca766a · GitHub		
Segfault in `QuantizedMatMul` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-689c-r7h2-fv9v

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-2022-35973 : TensorFlow is an open source platform for machine learning. If `QuantizedMatMul` is given nonscala… twitter.com/i/web/status/1…	2022-09-16 21:03:17
/r/netcve	CVE-2022-35973	2022-09-16 21:38:44

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

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