



CVE-2022-36005

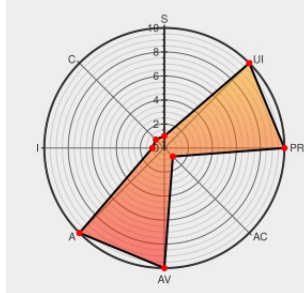
Published on: Not Yet Published

Last Modified on: 09/20/2022 02:42:00 PM UTC

CVE-2022-36005 - advisory for GHSA-r26c-679w-mrjm

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

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H



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

TensorFlow is an open source platform for machine learning. When ``tf.quantization.fake_quant_with_min_max_vars.gradient`` receives input ``min`` or ``max`` that is nonscalar, it gives a ``CHECK`` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit [f3cf67ac5705f4f04721d15e485e192bb319feed](#). 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-2022-36005 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 IsScalar / IsVector (rank) checks to input min/max tensors for Fa... · tensorflow/tensorflow@f3cf67a · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/f3cf67ac5705f4f04721d15e485e192bb319fee

4

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:2.10:rc3:*:*:*:*:*:
```

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-36005 : TensorFlow is an open source platform for machine learning. When `tf.quantization.fake_quant_with_... twitter.com/i/web/status/1...	2022-09-16 22:22:08
 /r/netcve	CVE-2022-36005	2022-09-16 23:38:58

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#)