

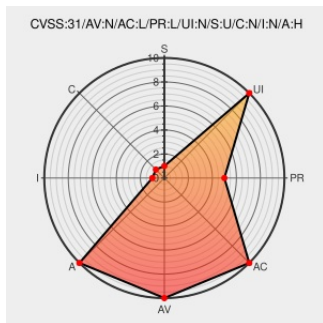


CVE-2022-23565

Published on: 02/04/2022 12:00:00 AM UTC

Last Modified on: 02/09/2022 05:38:00 PM UTC

CVE-2022-23565 - advisory for GHSA-4v5p-v5h9-6xjx

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

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

Tensorflow is an Open Source Machine Learning Framework. An attacker can trigger denial of service via assertion failure by altering a `SavedModel` on disk such that `AttrDef`s of some operation are duplicated. The fix will be included in TensorFlow 2.8.0. We will also cherry-pick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

CVE-2022-23565 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: tensorflow - tensorflow version $\geq 2.7.0$, $< 2.7.1$

Affected Vendor/Software: tensorflow - tensorflow version $\geq 2.6.0$, $< 2.6.3$

Affected Vendor/Software: tensorflow - tensorflow version $< 2.5.3$

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description

Tags

Link

`CHECK`-fail with repeated
`AttrDef` · Advisory ·
tensorflow/tensorflow · GitHub

github.com
text/html

CONFIRM

github.com/tensorflow/tensorflow/security/advisories/GHSA-4v5p-v5h9-6xjx

Remove a `DCHECK`-fail, log an
error instead. ·
tensorflow/tensorflow@c2b31ff ·
GitHub

github.com
text/html

MISC

github.com/tensorflow/tensorflow/commit/c2b31ff2d3151acb230edc3f5b1832d2c713a9e0

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

2.7.0

All

All

All

Application

Google

Tensorflow

All

All

All

All

Application

Google

Tensorflow

All

All

All

All

cpe:2.3:a:google:tensorflow:2.7.0:*****:

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source

Title

Posted (UTC)

@CVEreport

CVE-2022-23565 : Tensorflow is an Open Source Machine Learning Framework. An attacker can trigger denial of service... twitter.com/i/web/status/1...

2022-02-04
22:44:39

@LinInfoSec

Tensorflow - CVE-2022-23565: github.com/tensorflow/ten...

2022-02-05
02:00:15

← Previous ID

Next ID →

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](#)