



CVE-2022-36011

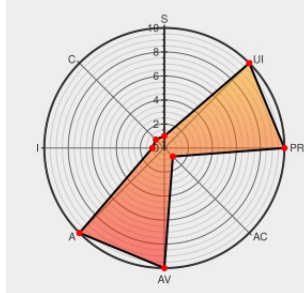
Published on: Not Yet Published

Last Modified on: 09/20/2022 02:40:00 PM UTC

CVE-2022-36011 - advisory for GHSA-fv43-93gv-vm8f

[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 ``mlir::tf::ConvertGenericFunctionToFunctionDef`` is given empty function attributes, it gives a null dereference. We have patched the issue in GitHub commit

[1cf45b831eeb0cab8655c9c7c5d06ec6f45fc41b](#). 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-2022-36011 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
[tf][functiondef_import] Emit error on empty function attributes · tensorflow/tensorflow@1cf45b8 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/1cf45b831eeb0cab8655c9c7c5d06ec6f45fc41b

GitHub

Null dereference on MLIR on empty function attributes · Advisory · tensorflow/tensorflow · GitHub

github.com

text/html

CONFIRM

github.com/tensorflow/tensorflow/security/advisories/GHSA-fv43-93gv-vm8f

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	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-2022-36011 : TensorFlow is an open source platform for machine learning. When `mlir::tf::ConvertGenericFuncio... twitter.com/i/web/status/1...	2022-09-16 22:41:20
/r/netcve	CVE-2022-36011	2022-09-16 23:39:03

← 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](#)