



CVE-2021-29590

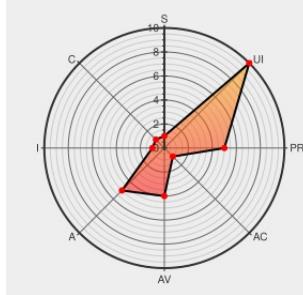
Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 05/19/2021 03:04:00 PM UTC

CVE-2021-29590 - advisory for GHSA-24x6-8c7m-hv3f

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

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



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

TensorFlow is an end-to-end open source platform for machine learning. The implementations of the `Minimum` and `Maximum` TFLite operators can be used to read data outside of bounds of heap allocated objects, if any of the two input tensor arguments are empty.

This is because the broadcasting

implementation(<https://github.com/tensorflow/tensorflow/blob/0d45ea1ca641b21b73bcf9c00e0L56>) indexes in both tensors with the same index but does not validate that the index is within bounds. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE-2021-29590 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: tensorflow - tensorflow version < 2.1.4

Affected Vendor/Software: tensorflow - tensorflow version >= 2.2.0, < 2.2.3

Affected Vendor/Software: tensorflow - tensorflow version >= 2.3.0, < 2.3.3

Affected Vendor/Software: tensorflow - tensorflow version >= 2.4.0, < 2.4.2

CVSS3 Score: **7.1 - HIGH**

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

CVSS2 Score: **3.6 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
Prevent a null pointer exception in TFLite · tensorflow/tensorflow@953f28d · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/953f28dca13c92839ba389c055587cfe6c723578
Heap OOB read in TFLite's implementation of `Minimum` or `Maximum` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-24x6-8c7m-hv3f

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.

Related QID Numbers

[982463](#) Python (pip) Security Update for tensorflow (GHSA-24x6-8c7m-hv3f)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
cpe:2.3:a:google:tensorflow:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)

[site](#). This site includes MITRE data granted under the following [license](#).

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