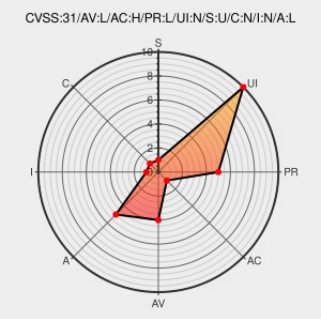
CVE-2021-29557

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

Last Modified on: 05/18/2021 07:59:00 PM UTC

CVE-2021-29557 - advisory for GHSA-xw93-v57j-fcgh

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tensorflow from Google contain the following vulnerability:

TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a denial of service via a FPE runtime error in `tf.raw_ops.SparseMatMul`. The division by 0 occurs deep in Eigen code because the `b` tensor is empty. The fix will be included in TensorFlow 2.5.0. We will also cherrypick 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-2021-29557 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM 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: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Fix FPE issue in external Eigen source code issue with `tf.raw_ops.Sp… · tensorflow/tensorflow@7f283ff · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/7f283ff806b2031f407db64c4d3edcda8fb9f9f5
Division by 0 in `SparseMatMul` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-xw93-v57j-fcgh

Related QID Numbers

982492 Python (pip) Security Update for tensorflow-gpu (GHSA-xw93-v57j-fcgh)

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)
@CVEreport	CVE-2021-29557 : TensorFlow is an end-to-end open source platform for machine learning. An attacker can cause a den… twitter.com/i/web/status/1…	2021-05-14 20:08:48
/r/netcve	CVE-2021-29557	2021-05-14 20:41:10

← Previous ID

Next ID→

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