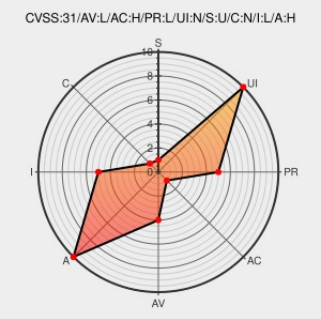
CVE-2021-29607

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

Last Modified on: 05/18/2021 03:08:00 PM UTC

CVE-2021-29607 - advisory for GHSA-gv26-jpj9-c8gq

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. Incomplete validation in `SparseAdd` results in allowing attackers to exploit undefined behavior (dereferencing null pointers) as well as write outside of bounds of heap allocated data. The implementation(https://github.com/tensorflow/tensorflow/blob/656e7673b14acd7835dc778867f8 has a large set of validation for the two sparse tensor inputs (6 tensors in total), but does not validate that the tensors are not empty or that the second dimension of `*_indices` matches the size of corresponding `*_shape`. This allows attackers to send tensor triples that represent invalid sparse tensors to abuse code assumptions that are not protected by validation. 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-2021-29607 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: 7.8 - HIGH

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

UNCHANGED HIGH HIGH HIGH

CVSS2 Score: 4.6 - MEDIUM

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

CVE References

Description	Tags	Link
Incomplete validation in `SparseSparseMinimum` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-gv26-jpj9-c8g
Validate that a and b are proper sparse tensors · tensorflow/tensorflow@f6fde89 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/f6fde895ef9c77d848061c0517f19d0ec2682f3a
Fix OOB issue with `tf.raw_ops.SparseSparseMinimum`. · tensorflow/tensorflow@ba6822b · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/ba6822bd7b7324ba201a28b2f278c29a98edbe

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID Next ID→

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