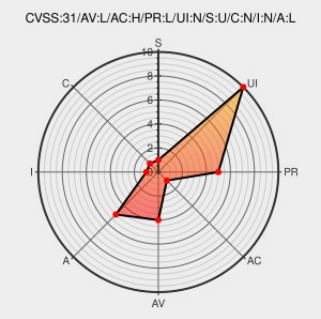
CVE-2021-29567

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

Last Modified on: 05/19/2021 07:36:00 PM UTC

CVE-2021-29567 - advisory for GHSA-wp3c-xw9g-gpcg

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. Due to lack of validation in `tf.raw_ops.SparseDenseCwiseMul`, an attacker can trigger denial of service via `CHECK`-fails or accesses to outside the bounds of heap allocated data. Since the implementation(https://github.com/tensorflow/tensorflow/blob/38178a2f7a681a7835bb0912702L80) only validates the rank of the input arguments but no constraints between dimensions(https://www.tensorflow.org/api_docs/python/tf/raw_ops/SparseDenseCwiseMul), an attacker can abuse them to trigger internal `CHECK` assertions (and cause program termination, denial of service) or to write to memory outside of bounds of heap allocated tensor buffers. 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-2021-29567 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**	**Integrity**	**Availability**

	Impact	Impact	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
Lack of validation in `SparseDenseCwiseMul` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-wp3c-xw9g-gpcg
Fix heap-buffer-overflow issue with `tf.raw_ops.SparseDenseCwiseMul`. · tensorflow/tensorflow@7ae2af3 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/7ae2af34087fb4b5c8915279efd03da3b81028b

Related QID Numbers

982482 Python (pip) Security Update for tensorflow-gpu (GHSA-wp3c-xw9g-gpcg)

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