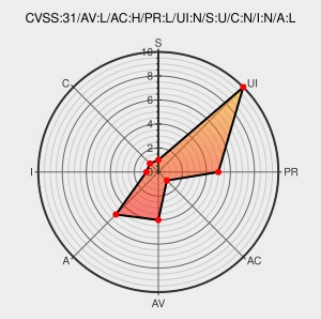
CVE-2021-29575

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

Last Modified on: 10/25/2022 07:56:00 PM UTC

CVE-2021-29575 - advisory for GHSA-6qgm-fv6v-rfpv

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. The implementation of `tf.raw_ops.ReverseSequence` allows for stack overflow and/or `CHECK`-fail based denial of service. The implementation(https://github.com/tensorflow/tensorflow/blob/5b3b071975e01f0d250c928b2a8 L118) fails to validate that `seq_dim` and `batch_dim` arguments are valid. Negative values for `seq_dim` can result in stack overflow or `CHECK`-failure, depending on the version of Eigen code used to implement the operation. Similar behavior can be exhibited by invalid values of `batch_dim`. 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-2021-29575 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
Add missing validations to reverse_sequence_op · tensorflow/tensorflow@ecf768c · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/ecf768cbe50cedc0a45ce1ee223146a3d3d26d23
Overflow/denial of service in `tf.raw_ops.ReverseSequence` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-6qgm-fv6v-rfpv

Related QID Numbers

982474 Python (pip) Security Update for tensorflow-gpu (GHSA-6qgm-fv6v-rfpv)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	All	All	All	All

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2021-29575	2021-05-14 19:41:21

← Previous ID

Next ID→