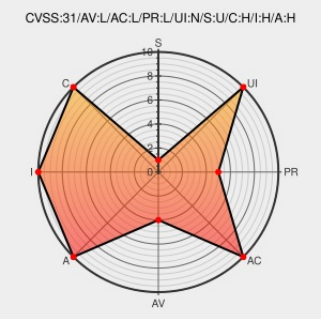
CVE-2021-37667

Published on: 08/12/2021 12:00:00 AM UTC

Last Modified on: 08/18/2021 08:49:00 PM UTC

CVE-2021-37667 - advisory for GHSA-w74j-v8xh-3w5h

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. In affected versions an attacker can cause undefined behavior via binding a reference to null pointer in `tf.raw_ops.UnicodeEncode`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/ L539) reads the first dimension of the `input_splits` tensor before validating that this tensor is not empty. We have patched the issue in GitHub commit 2e0ee46f1a47675152d3d865797a18358881d7a6. The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.

CVE-2021-37667 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.5.0, < 2.5.1**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.4.0, < 2.4.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 2.3.4**

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
Reference binding to nullptr in unicode encoding · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-w74j-v8xh-3w5h
Ensure non-empty input_splits in tf.raw_ops.UnicodeEncode · tensorflow/tensorflow@2e0ee46 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/2e0ee46f1a47675152d3d865797a18358881d7a6

Related QID Numbers

981536 Python (pip) Security Update for tensorflow-gpu (GHSA-w74j-v8xh-3w5h)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.5.0	All	All	All
Application	Google	Tensorflow	2.6.0	rc0	All	All
Application	Google	Tensorflow	2.6.0	rc1	All	All
Application	Google	Tensorflow	2.6.0	rc2	All	All

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

cpe:2.3:a:google:tensorflow:2.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.6.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.6.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.6.0:rc2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

@CVEreport	CVE-2021-37667 : TensorFlow is an end-to-end open source platform for machine learning. In affected versions an att… twitter.com/i/web/status/1…	2021-08-12 21:47:32
@LinInfoSec	Tensorflow - CVE-2021-37667: github.com/tensorflow/ten…	2021-08-13 00:52:16

← Previous ID

Next ID→