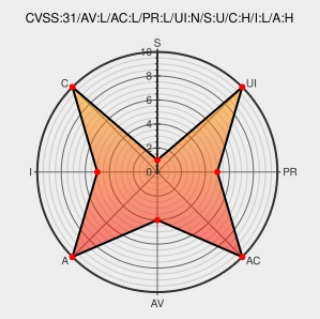
CVE-2021-37641

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

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

CVE-2021-37641 - advisory for GHSA-9c8h-vvrj-w2p8

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 if the arguments to `tf.raw_ops.RaggedGather` don't determine a valid ragged tensor code can trigger a read from outside of bounds of heap allocated buffers. The [implementation](https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/ directly reads the first dimension of a tensor shape before checking that said tensor has rank of at least 1 (i.e., it is not a scalar). Furthermore, the implementation does not check that the list given by `params_nested_splits` is not an empty list of tensors. We have patched the issue in GitHub commit a2b743f6017d7b97af1fe49087ae15f0ac634373. 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-2021-37641 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: 7.1 - HIGH

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

CVSS2 Score: 3.6 - LOW

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

CVE References

Description	Tags	Link
Fix heap OOB in `tf.raw_ops.RaggedGather` · tensorflow/tensorflow@a2b743f · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/a2b743f6017d7b97af1fe49087ae15f0ac634373
Heap OOB in `RaggedGather` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-9c8h-vvrj-w2p8

Related QID Numbers

981510 Python (pip) Security Update for tensorflow-gpu (GHSA-9c8h-vvrj-w2p8)

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-2021-37641 : TensorFlow is an end-to-end open source platform for machine learning. In affected versions if the… twitter.com/i/web/status/1…	2021-08-12 20:36:19
@LinInfoSec	Tensorflow - CVE-2021-37641: github.com/tensorflow/ten…	2021-08-12 22:40:40

← Previous ID

Next ID→