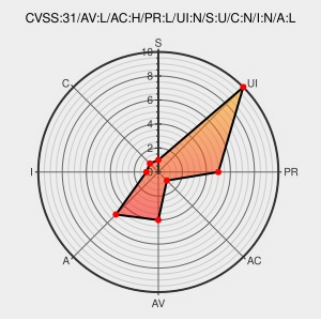
CVE-2021-29516

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

Last Modified on: 05/20/2021 04:05:00 PM UTC

CVE-2021-29516 - advisory for GHSA-84mw-34w6-2q43

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. Calling `tf.raw_ops.RaggedTensorToVariant` with arguments specifying an invalid ragged tensor results in a null pointer dereference. The implementation of `RaggedTensorToVariant` operations(https://github.com/tensorflow/tensorflow/blob/904b3926ed1c6c70380d5313d282d24 L40) does not validate that the ragged tensor argument is non-empty. Since `batched_ragged` contains no elements, `batched_ragged.splits` is a null vector, thus `batched_ragged.splits(0)` will result in dereferencing `nullptr`. 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-2021-29516 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
Fix `tf.raw_ops.RaggedTensorToVariant` invalid resize. · tensorflow/tensorflow@b055b9c · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/b055b9c474cd376259dde8779908f9eeaf097d
Null pointer dereference via invalid Ragged Tensors · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-84mw-34w6-2q43

Related QID Numbers

982530 Python (pip) Security Update for tensorflow-gpu (GHSA-84mw-34w6-2q43)

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)
@CVEreport	CVE-2021-29516 : TensorFlow is an end-to-end open source platform for machine learning. Calling `tf.raw_ops.RaggedT… twitter.com/i/web/status/1…	2021-05-14 20:08:02
/r/netcve	CVE-2021-29516	2021-05-14 20:41:08

← Previous ID

Next ID→

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