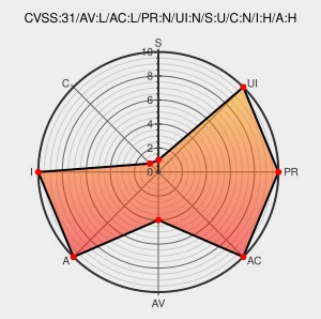
CVE-2021-37647

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

Last Modified on: 08/18/2021 04:25:00 PM UTC

CVE-2021-37647 - advisory for GHSA-c5x2-p679-95wc

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. When a user does not supply arguments that determine a valid sparse tensor, `tf.raw_ops.SparseTensorSliceDataset` implementation can be made to dereference a null pointer. The [implementation] (https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/L251) has some argument validation but fails to consider the case when either `indices` or `values` are provided for an empty sparse tensor when the other is not. If `indices` is empty, then [code that performs validation] (https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/L261) (i.e., checking that the indices are monotonically increasing) results in a null pointer dereference. If `indices` as provided by the user is empty, then `indices` in the C++ code above is backed by an empty `std::vector`, hence calling `indices->dim_size(0)` results in null pointer dereferencing (same as calling `std::vector::at()` on an empty vector). We have patched the issue in GitHub commit 02cc160e29d20631de3859c6653184e3f876b9d7. 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-2021-37647 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM 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: 5.5 - MEDIUM

Attack	Attack	Privileges	User

Vector	Complexity	Required	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
Prevent nullptr deref in SparseTensorSliceDataset · tensorflow/tensorflow@02cc160 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/02cc160e29d20631de3859c6653184e3f876b9d7
Null pointer dereference in `SparseTensorSliceDataset` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-c5x2-p679-95wc

Related QID Numbers

981516 Python (pip) Security Update for tensorflow-gpu (GHSA-c5x2-p679-95wc)

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-2021-37647 : TensorFlow is an end-to-end open source platform for machine learning. When a user does not supply… twitter.com/i/web/status/1…	2021-08-12 18:35:15

← Previous ID

Next ID→