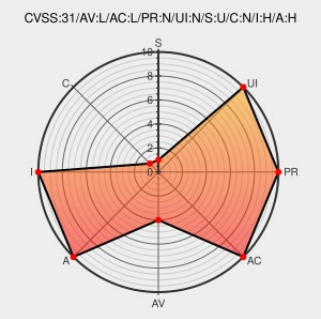
CVE-2021-37637

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

Last Modified on: 08/18/2021 05:20:00 PM UTC

CVE-2021-37637 - advisory for GHSA-c9qf-r67m-p7cg

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. It is possible to trigger a null pointer dereference in TensorFlow by passing an invalid input to `tf.raw_ops.CompressElement`. The [implementation](https://github.com/tensorflow/tensorflow/blob/47a06f40411a69c99f381495f490536972152ac0/ was accessing the size of a buffer obtained from the return of a separate function call before validating that said buffer is valid. We have patched the issue in GitHub commit 5dc7f6981fdaf74c8c5be41f393df705841fb7c5. 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-2021-37637 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 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	Access	Authentication

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

CVE References

Description	Tags	Link
Fix accessing possible nullptr in tensorflow::data::CompressElement a… · tensorflow/tensorflow@5dc7f69 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/5dc7f6981fdaf74c8c5be41f393df705841fb7c5
Null pointer dereference in `CompressElement` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-c9qf-r67m-p7cg

Related QID Numbers

981506 Python (pip) Security Update for tensorflow-gpu (GHSA-c9qf-r67m-p7cg)

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-2021-37637 : TensorFlow is an end-to-end open source platform for machine learning. It is possible to trigger a… twitter.com/i/web/status/1…	2021-08-12 18:33:41

← Previous ID

Next ID→