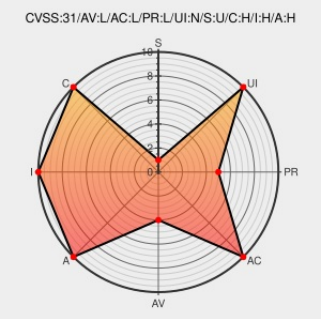
CVE-2021-37648

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

Last Modified on: 08/18/2021 08:57:00 PM UTC

CVE-2021-37648 - advisory for GHSA-wp77-4gmm-7cq8

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 the code for `tf.raw_ops.SaveV2` does not properly validate the inputs and an attacker can trigger a null pointer dereference. The [implementation] (https://github.com/tensorflow/tensorflow/blob/8d72537c6abf5a44103b57b9c2e22c14f5f49698/ uses `ValidateInputs` to check that the input arguments are valid. This validation would have caught the illegal state represented by the reproducer above. However, the validation uses `OP_REQUIRES` which translates to setting the `Status` object of the current `OpKernelContext` to an error status, followed by an empty `return` statement which just terminates the execution of the function it is present in. However, this does not mean that the kernel execution is finalized: instead, execution continues from the next line in `Compute` that follows the call to `ValidateInputs`. This is equivalent to lacking the validation. We have patched the issue in GitHub commit 9728c60e136912a12d99ca56e106b7cce7af5986. 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-2021-37648 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
Incorrect validation of `SaveV2` inputs · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-wp77-4gmm-7cq8
Ensure validation sticks in `save_restore_v2_ops.cc` · tensorflow/tensorflow@9728c60 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/9728c60e136912a12d99ca56e106b7cce7af5986

Related QID Numbers

981517 Python (pip) Security Update for tensorflow-gpu (GHSA-wp77-4gmm-7cq8)

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-2021-37648 : TensorFlow is an end-to-end open source platform for machine learning. In affected versions the co… twitter.com/i/web/status/1…	2021-08-12 21:21:09

← Previous ID

Next ID→