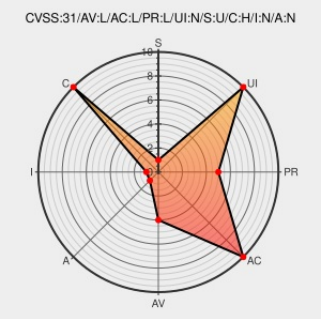
CVE-2021-37672

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

Last Modified on: 08/19/2021 02:28:00 PM UTC

CVE-2021-37672 - advisory for GHSA-5hj3-vjjf-f5m7

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 an attacker can read from outside of bounds of heap allocated data by sending specially crafted illegal arguments to `tf.raw_ops.SdcaOptimizerV2`. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/sdca_ops.cc#L353) does not check that the length of `example_labels` is the same as the number of examples. We have patched the issue in GitHub commit a4e138660270e7599793fa438cd7b2fc2ce215a6. 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-2021-37672 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	HIGH	NONE	NONE

CVSS2 Score: 2.1 - LOW

Access	Access	Authentication

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

CVE References

Description	Tags	Link
Heap OOB in `SdcaOptimizerV2` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-5hj3-vjjf-f5m7
Add remaining validation to `sdca_internal.cc` · tensorflow/tensorflow@a4e1386 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/a4e138660270e7599793fa438cd7b2fc2ce215a6

Related QID Numbers

981541 Python (pip) Security Update for tensorflow-gpu (GHSA-5hj3-vjjf-f5m7)

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)
@LinInfoSec	Tensorflow - CVE-2021-37672: github.com/tensorflow/ten…	2021-08-13 00:52:09

← Previous ID

Next ID→