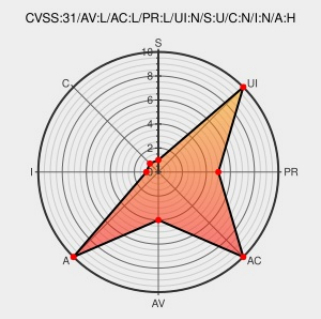
CVE-2021-37669

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

Last Modified on: 08/19/2021 02:27:00 PM UTC

CVE-2021-37669 - advisory for GHSA-vmjw-c2vp-p33c

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 cause denial of service in applications serving models using `tf.raw_ops.NonMaxSuppressionV5` by triggering a division by 0. The [implementation] (https://github.com/tensorflow/tensorflow/blob/460e000de3a83278fb00b61a16d161b1964f15f4/tensorflow/core/kernels/image_ops.cc#L271) uses a user controlled argument to resize a `std::vector`. However, as `std::vector::resize` takes the size argument as a `size_t` and `output_size` is an `int`, there is an implicit conversion to unsigned. If the attacker supplies a negative value, this conversion results in a crash. A similar issue occurs in `CombinedNonMaxSuppression`. We have patched the issue in GitHub commit 3a7362750d5c372420aa8f0caf7bf5b5c3d0f52d and commit [b5cdbf12ffcaaffecf98f22a6be5a64bb96e4f58. 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-2021-37669 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 Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Prevent crash/heap OOB due to integer conversion to unsigned in NMS k… · tensorflow/tensorflow@3a73627 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/3a7362750d5c372420aa8f0caf7bf5b5c3d0f52d
Prevent overflow due to integer conversion to unsigned. · tensorflow/tensorflow@b5cdbf1 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/b5cdbf12ffcaaffecf98f22a6be5a64bb96e4f58
Crash in NMS ops caused by integer conversion to unsigned · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-vmjw-c2vp-p33c

Related QID Numbers

981538 Python (pip) Security Update for tensorflow-gpu (GHSA-vmjw-c2vp-p33c)

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-2021-37669 : TensorFlow is an end-to-end open source platform for machine learning. In affected versions an att… twitter.com/i/web/status/1…	2021-08-12 23:04:33
@LinInfoSec	Tensorflow - CVE-2021-37669: github.com/tensorflow/ten…	2021-08-13 00:52:09

← Previous ID

Next ID→