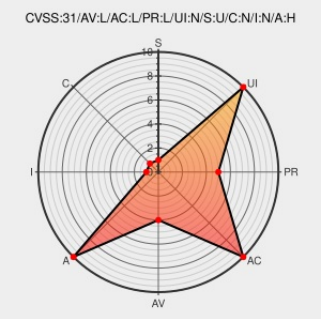
CVE-2021-41213

Published on: 11/05/2021 12:00:00 AM UTC

Last Modified on: 10/20/2022 09:25:00 PM UTC

CVE-2021-41213 - advisory for GHSA-h67m-xg8f-fxcf

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tensorflow from Google contain the following vulnerability:

TensorFlow is an open source platform for machine learning. In affected versions the code behind `tf.function` API can be made to deadlock when two `tf.function` decorated Python functions are mutually recursive. This occurs due to using a non-reentrant `Lock` Python object. Loading any model which contains mutually recursive functions is vulnerable. An attacker can cause denial of service by causing users to load such models and calling a recursive `tf.function`, although this is not a frequent scenario. The fix will be included in TensorFlow 2.7.0. We will also cherrypick this commit on TensorFlow 2.6.1, TensorFlow 2.5.2, and TensorFlow 2.4.4, as these are also affected and still in supported range.

CVE-2021-41213 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.6.0, < 2.6.1**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.5.0, < 2.5.2**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 2.4.4**

CVSS3 Score: 5.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication

NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Deadlock in mutually recursive `tf.function` objects · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-h67m-xg8f-fxcf
Fix the deadlock issue of recursive tf.function. · tensorflow/tensorflow@afac815 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/afac8158d43691661ad083f6dd9e56f327c1dcb7

Related QID Numbers

980178 Python (pip) Security Update for tensorflow-gpu (GHSA-h67m-xg8f-fxcf)

Exploit/POC from Github

TensorFlow is an open source platform for machine learning. In affected versions the code behind `tf.function` API ca…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.7.0	rc0	All	All
Application	Google	Tensorflow	2.7.0	rc1	All	All

cpe:2.3:a:google:tensorflow:*:*:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.7.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.7.0:rc1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@r3pwnx	CVE-2021-41213: Boring Deadlock in the Tensorflow < 2.6 https://t.co/ddqi9aCgs6	2021-11-05

@r3pwnx	CVE-2021-41213: Boring DeadLock in the Tensorflow<=2.6 https://t.co/ddoj96Ggs6	2021-11-05 07:12:32
@CVEreport	CVE-2021-41213 : TensorFlow is an open source platform for machine learning. In affected versions the code behind `… twitter.com/i/web/status/1…	2021-11-05 22:17:57

← Previous ID

Next ID→