

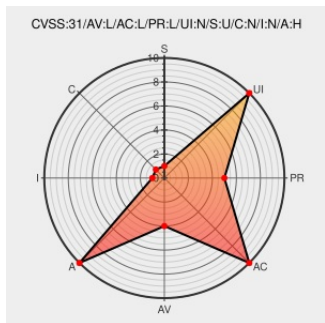


CVE-2021-41213

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 cherry-pick 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/afac815d43691661ad083f6dd9e56f327c1dcb7

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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)
@2surya	CVE-2021-41012: PoCing Deadlock in the Tensorflow - 2.6 https://t.co/dda9aCn6	2021-11-05

 @t3pwnix	CVE-2021-41213: Boring DeadLock in the TensorFlow<=2.6 https://t.co/du0j90Ggso	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→](#)

© CVE.report 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)