

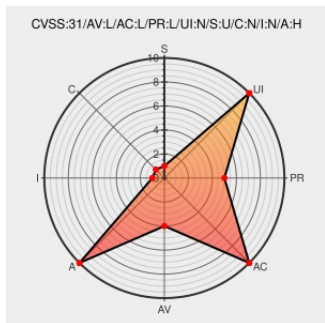


CVE-2021-41217

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

Last Modified on: 11/17/2021 09:38:18 PM UTC

CVE-2021-41217 - advisory for GHSA-5crj-c72x-m7gq

[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 process of building the control flow graph for a TensorFlow model is vulnerable to a null pointer exception when nodes that should be paired are not. This occurs because the code assumes that the first node in the pairing (e.g., an `Enter` node) always exists

when encountering the second node (e.g., an `Exit` node). When this is not the case, `parent` is `nullptr` so dereferencing it causes a crash. 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-2021-41217 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: tensorflow - tensorflow version $\geq 2.6.0$, $< 2.6.1$

Affected Vendor/Software: tensorflow - tensorflow version $\geq 2.5.0$, $< 2.5.2$

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

CVSS3 Score: **5.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	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

NONE

Integrity Impact

NONE

Availability Impact

PARTIAL

CVE References

Description	Tags	Link
Fix a NPE issue in invalid Exit op. Now it will report an error inste... · tensorflow/tensorflow@05cbebd · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/05cbebd3c6bb8f517a158b0155debb8df79017ff
Null pointer exception when `Exit` node is not preceded by `Enter` op · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-5crj-c72x-m7gq

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

980182 Python (pip) Security Update for tensorflow-gpu (GHSA-5crj-c72x-m7gq)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.6.0	All	All	All

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

cpe:2.3:a:google:tensorflow:2.6.0:*****:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41217 : TensorFlow is an open source platform for machine learning. In affected versions the process of bu... twitter.com/i/web/status/1...	2021-11-05 21:02:50

← Previous ID

Next ID →

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](#)