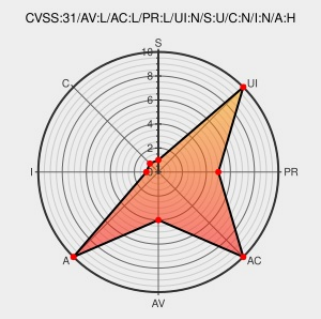
CVE-2021-41217

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 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-2021-41217 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	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
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

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→

CVE.report and Source URL Uptime Status status.cve.report