

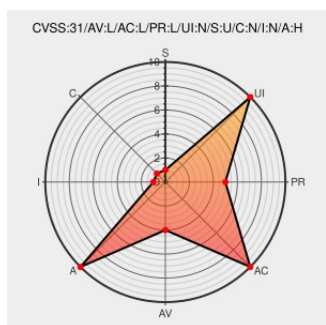


CVE-2021-41215

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

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

CVE-2021-41215 - advisory for GHSA-x3v8-c8qx-3j3r

[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 shape inference code for `DeserializeSparse` can trigger a null pointer dereference. This is because the shape inference function assumes that the `serialize\_sparse` tensor is a tensor with positive rank (and having `3` as the last dimension). 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-2021-41215 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	Integrity	Availability

Confidentiality Impact

NONE

Integrity Impact

NONE

Availability Impact

PARTIAL

CVE References

Description	Tags	Link
Ensuring that the input to DeserializeSparse is not a scalar. · tensorflow/tensorflow@d3738dd · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/d3738dd70f1c9ceb547258cbb82d853da8771850
Null pointer exception in `DeserializeSparse` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-x3v8-c8qx-3j3r

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

980180 Python (pip) Security Update for tensorflow-gpu (GHSA-x3v8-c8qx-3j3r)

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-2021-41215 : TensorFlow is an open source platform for machine learning. In affected versions the shape inferen... twitter.com/i/web/status/1...	2021-11-05 21:02:24

← Previous ID

Next ID →

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](#)