

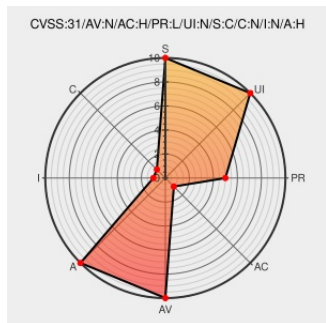


CVE-2020-15197

Published on: 09/25/2020 12:00:00 AM UTC

Last Modified on: 08/17/2021 01:21:00 PM UTC

CVE-2020-15197 - advisory for GHSA-qc53-44cj-vfvx

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Tensorflow](#) from [Google](#) contain the following vulnerability:

In Tensorflow before version 2.3.1, the ``SparseCountSparseOutput`` implementation does not validate that the input arguments form a valid sparse tensor. In particular, there is no validation that the ``indices`` tensor has rank 2. This tensor must be a matrix because code assumes its elements are accessed as elements of a matrix. However,

malicious users can pass in tensors of different rank, resulting in a ``CHECK`` assertion failure and a crash. This can be used to cause denial of service in serving installations, if users are allowed to control the components of the input sparse tensor. The issue is patched in commit `3cbb917b4714766030b28eba9fb41bb97ce9ee02` and is released in TensorFlow version 2.3.1.

CVE-2020-15197 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version = 2.3.0

CVSS3 Score: **6.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	NONE	NONE	HIGH

CVSS2 Score: **3.5 - LOW**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

NONE

PARTIAL

CVE References

Description	Tags	Link
Fix multiple vulnerabilities in <code>`tf.raw_ops.*CountSparseOutput`</code> . · tensorflow/tensorflow@3cbb917 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/tensorflow/tensorflow/commit/3cbb917b4714766030b28eba9fb41bb97c
Crash due to invalid splits in <code>SparseCountSparseOutput</code> . Advisory · tensorflow/tensorflow · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-qc53-44c
Release TensorFlow 2.3.1 · tensorflow/tensorflow · GitHub	Third Party Advisory github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.3.1

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

981470 Python (pip) Security Update for tensorflow-gpu (GHSA-qc53-44cj-vfvx)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	2.3.0	All	All	All
Application	Tensorflow	Tensorflow	2.3.0	All	All	All
Application	Tensorflow	Tensorflow	2.3.0	All	All	All

cpe:2.3:a:google:tensorflow:2.3.0:*:*:*:*:*:

cpe:2.3:a:tensorflow:tensorflow:2.3.0:*:*:*:*:*:

cpe:2.3:a:tensorflow:tensorflow:2.3.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
--------	-------	--------------

← Previous ID

Next ID →

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](#)