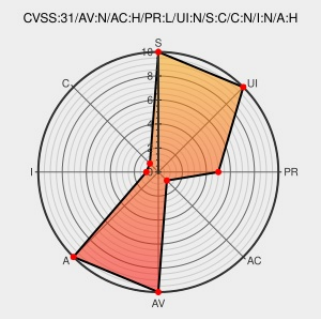
CVE-2020-15197

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 `tf.raw_ops.*CountSparseOutput`. · 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 SparseCountSparseOutput · 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

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→

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