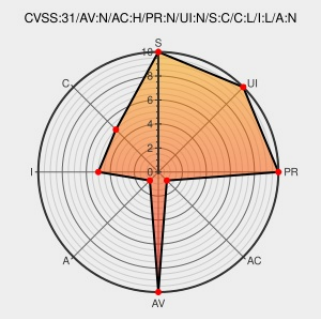
CVE-2020-15198

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

Last Modified on: 11/18/2021 05:22:00 PM UTC

CVE-2020-15198 - advisory for GHSA-jc87-6vpp-7ff3

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 the same shape as the `values` one. The values in these tensors are always accessed in parallel. Thus, a shape mismatch can result in accesses outside the bounds of heap allocated buffers. The issue is patched in commit 3cbb917b4714766030b28eba9fb41bb97ce9ee02 and is released in TensorFlow version 2.3.1.

CVE-2020-15198 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, < 2.3.1**

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

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
Heap buffer overflow due to invalid indices in SparseCountSparseOutput · Advisory · tensorflow/tensorflow · GitHub	Exploit Third Party Advisory github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-jc87-6vp
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

981472 Python (pip) Security Update for tensorflow-gpu (GHSA-jc87-6vpp-7ff3)

Known Affected Configurations (CPE V2.3)

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

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

cpe:2.3:a:tensorflow:tensorflow:*:*:*:*:-:*:*:*:

cpe:2.3:a:tensorflow:tensorflow:*:*:*:*:-:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Tensorflow - CVE-2020-15198: github.com/tensorflow/ten…	2021-08-17 14:46:20

← Previous ID

Next ID→

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