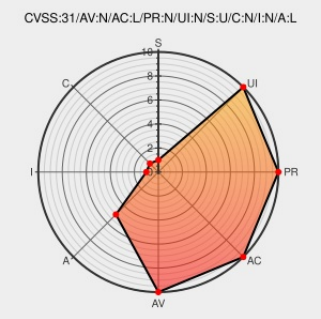
CVE-2020-15191

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

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

CVE-2020-15191 - advisory for GHSA-q8qj-fc9q-cphr

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tensorflow from Google contain the following vulnerability:

In Tensorflow before versions 2.2.1 and 2.3.1, if a user passes an invalid argument to `dlpack.to_dlpack` the expected validations will cause variables to bind to `nullptr` while setting a `status` variable to the error condition. However, this `status` argument is not properly checked. Hence, code following these methods will bind references to null pointers. This is undefined behavior and reported as an error if compiling with `-fsanitize=null`. The issue is patched in commit 22e07fb204386768e5bcbea563641ea11f96ceb8 and is released in TensorFlow versions 2.2.1, or 2.3.1.

CVE-2020-15191 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **= 2.2.0**

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

CVSS3 Score: 5.3 - MEDIUM

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality	**Integrity**	**Availability**

Impact	Impact	Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Fix multiple vulnerabilities in `tf.experimental.dlpack.to_dlpack`. · tensorflow/tensorflow@22e07fb · GitHub	Patch, Third Party Advisory, github.com, text/html	MISC github.com/tensorflow/tensorflow/commit/22e07fb204386768e5bcbea563641ea11f
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
Undefined behavior in dlpack · Advisory · tensorflow/tensorflow · GitHub	Exploit, Third Party Advisory, github.com, text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-q8qj-fc9
[security-announce] openSUSE-SU-2020:1766-1: moderate: Security update f	lists.opensuse.org, text/html	SUSE openSUSE-SU-2020:1766

Related QID Numbers

980050 Python (pip) Security Update for tensorflow-gpu (GHSA-q8qj-fc9q-cphr)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	2.2.0	All	All	All
Application	Google	Tensorflow	2.3.0	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Tensorflow	Tensorflow	2.2.0	All	All	All
Application	Tensorflow	Tensorflow	2.3.0	All	All	All
Application	Tensorflow	Tensorflow	2.2.0	All	All	All
Application	Tensorflow	Tensorflow	2.3.0	All	All	All

cpe:2.3:a:google:tensorflow:2.2.0:*:*:*:-:*:*:*:

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

cpe:2.3:o:opensuse:leap:15.2:*:*:*:*:*:*:*:

cpe:2.3:a:tensorflow:tensorflow:2.2.0:*:*:*:-:*:*:*:

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

cpe:2.3:a:tensorflow:tensorflow:2.2.0:*:*:*:-:*:*:*:

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Tensorflow - CVE-2020-15191: github.com/tensorflow/ten…	2021-08-17 14:46:21

← Previous ID

Next ID→