

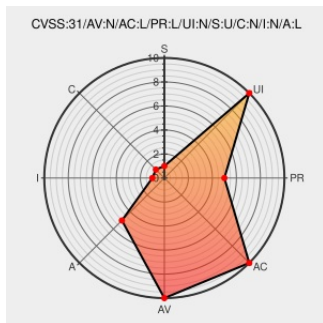


CVE-2020-15192

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

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

CVE-2020-15192 - advisory for GHSA-8fxw-76px-3rxv

[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 a list of strings to ``dlpack.to_dlpack`` there is a memory leak following an expected validation failure. The issue occurs because the ``status`` argument during validation failures is not properly checked. Since each of the above methods can return an error status, the ``status`` value

must be checked before continuing. The issue is patched in commit `22e07fb204386768e5bcbea563641ea11f96ceb8` and is released in TensorFlow versions 2.2.1, or 2.3.1.

CVE-2020-15192 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: **4.3 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

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

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.

981475 Python (pip) Security Update for tensorflow-gpu (GHSA-8fxw-76px-3rxv)

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)
--------	-------	--------------

← Previous ID

Next ID→