

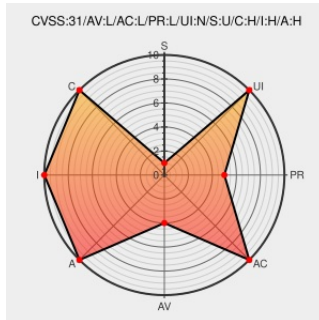


CVE-2021-41220

Published on: 11/05/2021 12:00:00 AM UTC

Last Modified on: 11/17/2021 09:38:18 PM UTC

CVE-2021-41220 - advisory for GHSA-gpvh-jvf9-7wg5

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

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

TensorFlow is an open source platform for machine learning. In affected versions the async implementation of `CollectiveReduceV2` suffers from a memory leak and a use after free. This occurs due to the asynchronous computation and the fact that objects that have been `std::move()`d from are still accessed. The fix will be included in TensorFlow 2.7.0. We will also cherry-pick this commit on TensorFlow 2.6.1, as this version is the only one that is also affected.

CVE-2021-41220 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: tensorflow - tensorflow version $\geq 2.6.0$, $< 2.6.1$

CVSS3 Score: **7.8 - HIGH**

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

CVSS2 Score: **4.6 - MEDIUM**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Fix undefined behavior in CollectiveReduceV2 and others · tensorflow/tensorflow@ca38dab · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/ca38dab9d3ee66c5de06f11af9a4b1200da5ef75
Use after free / memory leak in `CollectiveReduceV2` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-gpjh-jvf9-7wg5

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
980185 Python (pip) Security Update for tensorflow-gpu (GHSA-gpjh-jvf9-7wg5)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.7.0	rc0	All	All
Application	Google	Tensorflow	2.7.0	rc1	All	All
cpe:2.3:a:google:tensorflow:*:*:*:*:*:						
cpe:2.3:a:google:tensorflow:2.7.0:rc0:*:*:*:*:						
cpe:2.3:a:google:tensorflow:2.7.0:rc1:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
@CVEreport	CVE-2021-41220 : TensorFlow is an open source platform for machine learning. In affected versions the async impleme... twitter.com/i/web/status/1...	2021-11-05 22:23:01