

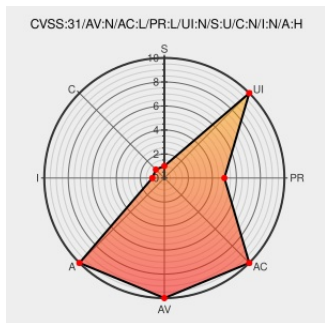


CVE-2022-21739

Published on: 02/03/2022 12:00:00 AM UTC

Last Modified on: 02/09/2022 05:23:00 AM UTC

CVE-2022-21739 - advisory for GHSA-3mw4-6rj6-74g5

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

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

Tensorflow is an Open Source Machine Learning Framework. The implementation of `QuantizedMaxPool` has an undefined behavior where user controlled inputs can trigger a reference binding to null pointer. The fix will be included in TensorFlow 2.8.0. We will also cherry-pick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

CVE-2022-21739 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Reference binding to null pointer in	github.com	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-3r

QuantizedMaxPool

Advisory

tensorflow/tensorflow

GitHub

github.com

text/html

tensorflow/quantized_pooling_ops.cc at 5100e359aef5c8021f2e71c7b986420b85ce7b3d

github.com

text/html

MISC

github.com/tensorflow/tensorflow/blob/5100e359aef5c8021f2e71c7b986420b85ce7b3d

L130

Fix nullptr exception in QuantizedMaxPool op when empty list is sent ...

github.com

text/html

MISC

github.com/tensorflow/tensorflow/commit/53b0dd6dc5957652f359653b0dd6dc5957652f3596

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	2.7.0	All	All	All
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	All	All	All	All

cpe:2.3:a:google:tensorflow:2.7.0:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-21739 : Tensorflow is an Open Source Machine Learning Framework. The implementation of QuantizedMaxPool ... twitter.com/i/web/status/1...	2022-02-03 13:21:56
/r/netcve	CVE-2022-21739	2022-02-03 14:38:51

Previous ID

Next ID

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web](#)

[site](#). This site includes MITRE data granted under the following [license](#).

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