



CVE-2022-41884

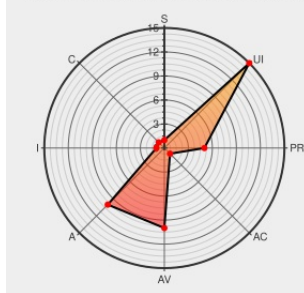
Published on: Not Yet Published

Last Modified on: 11/22/2022 09:53:00 PM UTC

CVE-2022-41884 - advisory for GHSA-jq6x-99hj-q636

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

CVSS:31/AV:N/AC:H/PR:L/UI:R/S:U/C:N/I:N/A:H



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

TensorFlow is an open source platform for machine learning. If a numpy array is created with a shape such that one element is zero and the others sum to a large number, an error will be raised. We have patched the issue in GitHub commit

2b56169c16e375c521a3bc8ea658811cc0793784. The fix will be

included in TensorFlow 2.11. We will also cherry-pick this commit on TensorFlow 2.10.1, 2.9.3, and TensorFlow 2.8.4, as these are also affected and still in supported range.

CVE-2022-41884 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version $\geq 2.10.0$, $< 2.10.1$

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version $\geq 2.9.0$, $< 2.9.3$

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version $< 2.8.4$

CVSS3 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Fix segfault when using unusually shaped tensors. · tensorflow/tensorflow@2b56169 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/2b56169c16e375c521a3bc8ea658811cc0793784

Seg fault in
`ndarray\_tensor\_bridge` due to
zero and large inputs · Advisory
· tensorflow/tensorflow · GitHub

[github.com](#)
[text/html](#)

 **CONFIRM** github.com/tensorflow/tensorflow/security/advisories/GHSA-jq6x-99hj-q636

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

[904611](#) Common Base Linux Mariner (CBL-Mariner) Security Update for tensorflow (11525)

[904652](#) Common Base Linux Mariner (CBL-Mariner) Security Update for tensorflow (11525-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.10.0	All	All	All
cpe:2.3:a:google:tensorflow:*:*:*:*:*:						
cpe:2.3:a:google:tensorflow:2.10.0:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-41884 : TensorFlow is an open source platform for machine learning. If a numpy array is created with a sha... twitter.com/i/web/status/1...	2022-11-18 21:22:15
 /r/netcve	CVE-2022-41884	2022-11-18 22:38:26

[← 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](#)