

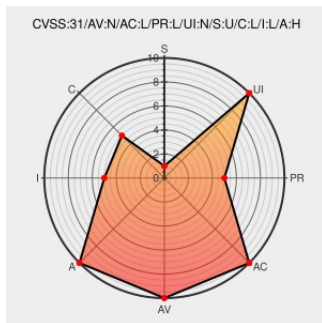


CVE-2022-21740

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

Last Modified on: 02/09/2022 05:36:00 AM UTC

CVE-2022-21740 - advisory for GHSA-44qp-9wwf-734r

[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 `SparseCountSparseOutput` is vulnerable to a heap overflow. 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-2022-21740 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

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

CVE References

Description	Tags	Link
Cleanup and remove duplicate validation in `SparseCount`.	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/2b7100d6cdf36aa21010

tensorflow/tensorflow@2b7100d · GitHub

Further validate sparse tensor for
`SparseCount`: indices must be val...
tensorflow/tensorflow@adbbabd · GitHub

github.com

text/html

MISC github.com/tensorflow/tensorflow/commit/adbbabdb0d3abb3cdeac

tensorflow/count_ops.cc at
5100e359aef5c8021f2e71c7b986420b85ce7b3d
· tensorflow/tensorflow · GitHub

github.com

text/html

MISC github.com/tensorflow/tensorflow/blob/5100e359aef5c8021f2e71c7b986420b85ce7b3d
L273

Heap overflow in `SparseCountSparseOutput` ·
Advisory · tensorflow/tensorflow · GitHub

github.com

text/html

CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-44

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-2022-21740 : Tensorflow is an Open Source Machine Learning Framework. The implementation of `SparseCountSparseO... twitter.com/i/web/status/1...	2022-02-03 14:41:04
/r/netcve	CVE-2022-21740	2022-02-03 15:38:31

← Previous ID

Next ID →

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](#)