



CVE-2023-25665

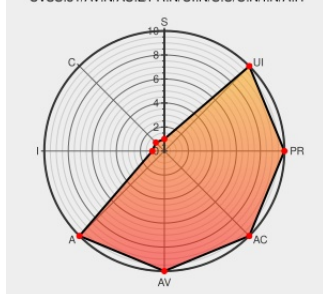
Published on: Not Yet Published

Last Modified on: 03/31/2023 02:20:00 PM UTC

CVE-2023-25665 - advisory for GHSA-558h-mq8x-7q9g

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

CVSS:31/AV:N/AC:L/PR:N/UI:N/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. Prior to versions 2.12.0 and 2.11.1, when `SparseSparseMaximum` is given invalid sparse tensors as inputs, it can give a null pointer error. A fix is included in TensorFlow version 2.12 and version 2.11.1.

CVE-2023-25665 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version = < 2.11.1

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
NPE in SparseSparseMaximum · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/security/advisories/GHSA-558h-mq8x-7q9g
Add validation checks in sparse binary ops. · tensorflow/tensorflow@5e0ecfb · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/5e0ecfb42f5f65629fd7a4edd6c4afe7ff0feb04

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

907413 Common Base Linux Mariner (CBL-Mariner) Security Update for tensorflow (31216-1)

Known Affected Configurations (CPE V2.3)

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 /r/netcve	CVE-2023-25665	2023-03-25 01:38:21

← Previous ID

Next ID→