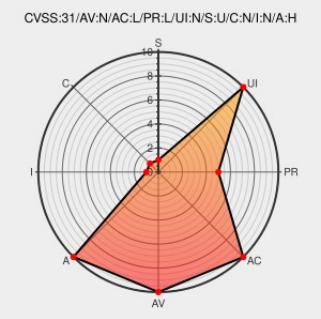
CVE-2023-25661

Published on: Not Yet Published

Last Modified on: 04/03/2023 04:19:00 PM UTC

CVE-2023-25661 - advisory for GHSA-fxgc-95xx-grvq

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. In versions prior to 2.11.1 a malicious invalid input crashes a tensorflow model (Check Failed) and can be used to trigger a denial of service attack. A proof of concept can be constructed with the `Convolution3DTranspose` function. This Convolution3DTranspose layer is a very common API in modern neural networks. The ML models containing such vulnerable components could be deployed in ML applications or as cloud services. This failure could be potentially used to trigger a denial of service attack on ML cloud services. An attacker must have privilege to provide input to a `Convolution3DTranspose` call. This issue has been patched and users are advised to upgrade to version 2.11.1. There are no known workarounds for this vulnerability.

CVE-2023-25661 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **= < 2.11.1**

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

CVE References

Description	Tags	Link
Fix nn.conv3d_transpose security vulnerability with illegal input	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/948fe6369a5711d4b4568ea9bbf6015c6dfb77e2

snape · tensorflow/tensorflow@948fe63 · GitHub

Denial of Service in TensorFlow · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/security/advisories/GHSA-fxgc-95xx-grvq

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

907394 Common Base Linux Mariner (CBL-Mariner) Security Update for tensorflow (31197)

907487 Common Base Linux Mariner (CBL-Mariner) Security Update for tensorflow (31197-1)

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)
@CVEreport	CVE-2023-25661 : TensorFlow is an Open Source Machine Learning Framework. In versions prior to 2.11.1 a malicious i… twitter.com/i/web/status/1…	2023-03-27 20:06:33
/r/netcve	CVE-2023-25661	2023-03-27 21:38:25

← Previous ID

Next ID→