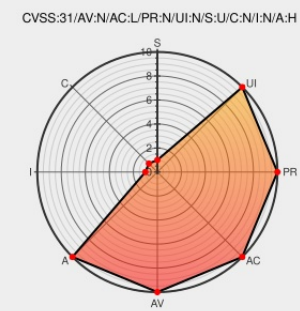
CVE-2023-25663

Published on: Not Yet Published

Last Modified on: 03/30/2023 05:42:00 PM UTC

CVE-2023-25663 - advisory for GHSA-64jg-wjww-7c5w

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



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 `ctx->step_containter()` is a null ptr, the Lookup function will be executed with a null pointer. A fix is included in TensorFlow 2.12.0 and 2.11.1.

CVE-2023-25663 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 TensorArrayConcatV2 · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/security/advisories/GHSA-64jg-wjww-7c5w
Fixing null pointer read in TensorArrayConcat when the step container… · tensorflow/tensorflow@239139d · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/239139d2ae6a81ae9ba499ad78b56d9b2931538a

comment@cve.report.

Related QID Numbers

907391 Common Base Linux Mariner (CBL-Mariner) Security Update for tensorflow (31215-1)

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-2023-25663	2023-03-25 01:38:20

← Previous ID

Next ID→