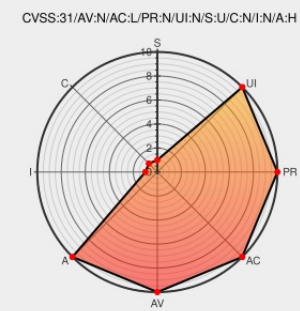
CVE-2023-25667

Published on: Not Yet Published

Last Modified on: 11/07/2023 04:09:00 AM UTC

CVE-2023-25667 - advisory for GHSA-fqm2-gh8w-gr68

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, integer overflow occurs when `2^31 <= num_frames * height * width * channels < 2^32`, for example Full HD screencast of at least 346 frames. A fix is included in TensorFlow version 2.12.0 and version 2.11.1.

CVE-2023-25667 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
Fix integer overflow for multiframe gifs. · tensorflow/tensorflow@8dc723f · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/8dc723fcdd1a6127d6c970bd2ecb18b019a1a58d
Segfault when opening multiframe gif · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/security/advisories/GHSA-fqm2-gh8w-gr68

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

907414 Common Base Linux Mariner (CBL-Mariner) Security Update for tensorflow (31198-1)

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-2023-25667	2023-03-25 01:38:22

← Previous ID

Next ID→