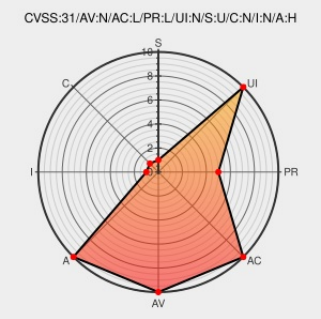
CVE-2022-21737

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

Last Modified on: 02/09/2022 05:08:00 AM UTC

CVE-2022-21737 - advisory for GHSA-f2vv-v9cg-qhh7

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 `*Bincount` operations allows malicious users to cause denial of service by passing in arguments which would trigger a `CHECK`-fail. There are several conditions that the input arguments must satisfy. Some are not caught during shape inference and others are not caught during kernel implementation. This results in `CHECK` failures later when the output tensors get allocated. The fix will be included in TensorFlow 2.8.0. We will also cherrypick 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-2022-21737 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

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

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
tensorflow/bincount_op.cc at 5100e359aef5c8021f2e71c7b986420b85ce7b3d · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/5100e359aef5c8021f2e71c7b986420b
Assertion failure based denial of service via faulty bin count operations · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-f2
Fix check-fail when bincount ops are passed invalid values. · tensorflow/tensorflow@7019ce4 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/7019ce4f68925fd01cdafd

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-2022-21737 : Tensorflow is an Open Source Machine Learning Framework. The implementation of `*Bincount` operati… twitter.com/i/web/status/1…	2022-02-03 13:50:22
/r/netcve	CVE-2022-21737	2022-02-03 14:38:54

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report