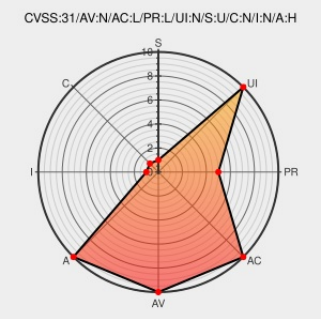
CVE-2022-23571

Published on: 02/04/2022 12:00:00 AM UTC

Last Modified on: 02/10/2022 04:08:00 PM UTC

CVE-2022-23571 - advisory for GHSA-j3mj-fhpq-qqjj

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. When decoding a tensor from protobuf, a TensorFlow process can encounter cases where a `CHECK` assertion is invalidated based on user controlled arguments, if the tensors have an invalid `dtype` and 0 elements or an invalid shape. This allows attackers to cause denial of services in TensorFlow processes. 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-2022-23571 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.7.0, < 2.7.1**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.6.0, < 2.6.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 2.5.3**

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	**Integrity**	**Availability**

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Validate `proto.dtype()` before calling `set_dtype()`. · tensorflow/tensorflow@5b491cd · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/5b491cd5e41ad63735161cec9c2a568172c8b6a3
`CHECK`-fail when decoding invalid tensors from proto · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-j3mj-fhpq-qqjj

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-2022-23571 : Tensorflow is an Open Source Machine Learning Framework. When decoding a tensor from protobuf, a T… twitter.com/i/web/status/1…	2022-02-04 22:45:41
@LinInfoSec	Tensorflow - CVE-2022-23571: github.com/tensorflow/ten…	2022-02-05 02:00:14

← Previous ID

Next ID→

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