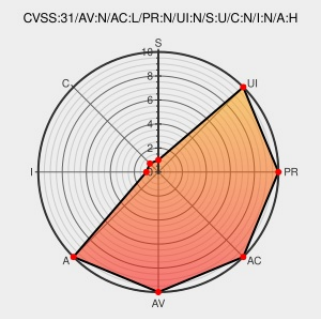
CVE-2022-23591

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

Last Modified on: 06/27/2023 02:40:00 AM UTC

CVE-2022-23591 - advisory for GHSA-247x-2f9f-5wp7

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 `GraphDef` format in TensorFlow does not allow self recursive functions. The runtime assumes that this invariant is satisfied. However, a `GraphDef` containing a fragment such as the following can be consumed when loading a `SavedModel`. This would result in a stack overflow during execution as resolving each `NodeDef` means resolving the function itself and its nodes. 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-2022-23591 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH 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: 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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Prevent stack overflow when FunctionLib in GraphDef has a self-recurs… · tensorflow/tensorflow@448a161 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/448a16182065bd08a202d9057dd8ca541e67996c
Stack overflow due to self-recursive function in `GraphDef` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-247x-2f9f-5wp7

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-2022-23591 : Tensorflow is an Open Source Machine Learning Framework. The `GraphDef` format in TensorFlow does… twitter.com/i/web/status/1…	2022-02-04 22:52:19
@LinInfoSec	Tensorflow - CVE-2022-23591: github.com/tensorflow/ten…	2022-02-05 02:00:13
/r/netcve	CVE-2022-23591	2022-02-04 23:38:48

← Previous ID

Next ID→