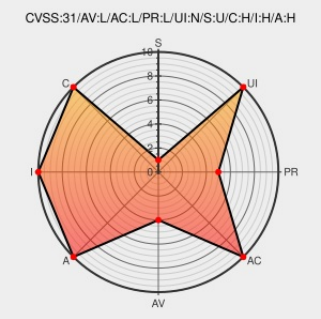
CVE-2022-29216

Published on: Not Yet Published

Last Modified on: 06/03/2022 02:47:00 AM UTC

CVE-2022-29216 - advisory for GHSA-75c9-jrh4-79mc

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 2.9.0, 2.8.1, 2.7.2, and 2.6.4, TensorFlow's `saved_model_cli` tool is vulnerable to a code injection. This can be used to open a reverse shell. This code path was maintained for compatibility reasons as the maintainers had several test cases where numpy expressions were used as arguments. However, given that the tool is always run manually, the impact of this is still not severe. The maintainers have now removed the `safe=False` argument, so all parsing is done without calling `eval`. The patch is available in versions 2.9.0, 2.8.1, 2.7.2, and 2.6.4.

CVE-2022-29216 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 2.6.4**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.7.0rc0, < 2.7.2**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.8.0rc0, < 2.8.1**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.9.0rc0, < 2.9.0**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication

LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Always do safe parsing · tensorflow/tensorflow@c5da7af · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/c5da7af048611aa29e9382
Release TensorFlow 2.8.1 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.8.1
Release TensorFlow 2.9.0 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.9.0
Release TensorFlow 2.7.2 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.7.2
Release TensorFlow 2.6.4 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.6.4
Code injection in `saved_model_cli` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-75
tensorflow/saved_model_cli.py at f3b9bf4c3c0597563b289c0512e98d4ce81f886e · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/f3b9bf4c3c0597563b289c0512e98d4c L574
Remove use of `eval` when evaluating the input example. · tensorflow/tensorflow@8b202f0 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/8b202f08d52e8206af2bdb

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	All	All	All	All
Application	Google	Tensorflow	2.7.0	rc0	All	All
Application	Google	Tensorflow	2.7.0	rc1	All	All
Application	Google	Tensorflow	2.8.0	-	All	All
Application	Google	Tensorflow	2.8.0	rc0	All	All
Application	Google	Tensorflow	2.8.0	rc1	All	All
Application	Google	Tensorflow	2.9.0	rc0	All	All
Application	Google	Tensorflow	2.9.0	rc1	All	All

Application	Google	TensorFlow	2.9.0	0rc1	All	All

cpe:2.3:a:google:tensorflow:*:*:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.7.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.7.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.8.0:-:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.8.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.8.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.9.0:rc0:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:2.9.0:rc1:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29216 : TensorFlow is an open source platform for machine learning. Prior to versions 2.9.0, 2.8.1, 2.7.2,… twitter.com/i/web/status/1…	2022-05-20 23:44:32
@LinInfoSec	Tensorflow - CVE-2022-29216: github.com/tensorflow/ten…	2022-05-21 06:00:53
/r/netcve	CVE-2022-29216	2022-05-21 00:38:15

← Previous ID

Next ID→