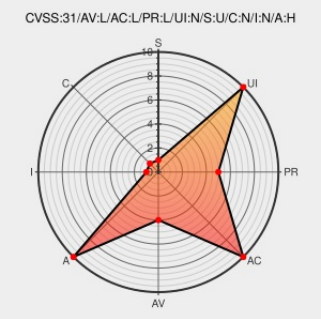
CVE-2022-29211

Published on: Not Yet Published

Last Modified on: 06/03/2022 03:02:00 PM UTC

CVE-2022-29211 - advisory for GHSA-xrp2-fhq4-4q3w

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, the implementation of `tf.histogram_fixed_width` is vulnerable to a crash when the values array contain `Not a Number` (`NaN`) elements. The implementation assumes that all floating point operations are defined and then converts a floating point result to an integer index. If `values` contains `NaN` then the result of the division is still `NaN` and the cast to `int32` would result in a crash. This only occurs on the CPU implementation. Versions 2.9.0, 2.8.1, 2.7.2, and 2.6.4 contain a patch for this issue.

CVE-2022-29211 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM 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: 5.5 - MEDIUM

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

CVSS2 Score: 2.1 - LOW

Access Vector	Access Complexity	Authentication

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

CVE References

Description	Tags	Link
Release TensorFlow 2.8.1 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.8.1
Segmentation fault in tf.histogram_fixed_width · Issue #45770 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/issues/45770
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
tensorflow/histogram_op.cc at f3b9bf4c3c0597563b289c0512e98d4ce81f886e · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/f3b9bf4c3c0597563b289c0512e98d4c L74
Release TensorFlow 2.6.4 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.6.4
tensorflow/histogram_op.cc at f3b9bf4c3c0597563b289c0512e98d4ce81f886e · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/f3b9bf4c3c0597563b289c0512e98d4c
Segfault if `tf.histogram_fixed_width` is called with NaN values · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-xrp
Prevent crash when histogram is called with NaN values. · tensorflow/tensorflow@e57fd69 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/e57fd691c7b0fd00ea3bfe4

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

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-2022-29211 : 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 23:22:12
@LinInfoSec	Tensorflow - CVE-2022-29211: github.com/tensorflow/ten…	2022-05-21 06:00:52
/r/netcve	CVE-2022-29211	2022-05-21 00:38:11

← Previous ID

Next ID→