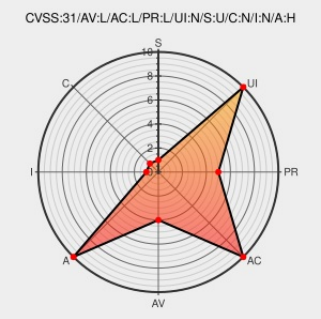
CVE-2022-29210

Published on: Not Yet Published

Last Modified on: 06/28/2023 08:26:00 PM UTC

CVE-2022-29210 - advisory for GHSA-hc2f-7r5r-r2hg

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. In version 2.8.0, the `TensorKey` hash function used total estimated `AllocatedBytes()`, which (a) is an estimate per tensor, and (b) is a very poor hash function for constants (e.g. `int32_t`). It also tried to access individual tensor bytes through `tensor.data()` of size `AllocatedBytes()`. This led to ASAN failures because the `AllocatedBytes()` is an estimate of total bytes allocated by a tensor, including any pointed-to constructs (e.g. strings), and does not refer to contiguous bytes in the `.data()` buffer. The discoverers could not use this byte vector anyway because types such as `tstring` include pointers, whereas they needed to hash the string values themselves. This issue is patched in Tensorflow versions 2.9.0 and 2.8.1.

CVE-2022-29210 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **== 2.8.0**

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
Release TensorFlow 2.9.0 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.9.0
Heap buffer overflow due to incorrect hash function · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-hc2
tensorflow/tensor_key.h at f3b9bf4c3c0597563b289c0512e98d4ce81f886e · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/f3b9bf4c3c0597563b289c0512e98d4c L64
Fix TensorKey hash function. · tensorflow/tensorflow@1b85a28 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/1b85a28d395dc91f4d22b5

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	2.8.0	All	All	All

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-29210 : TensorFlow is an open source platform for machine learning. In version 2.8.0, the `TensorKey` hash… twitter.com/i/web/status/1…	2022-05-20 23:33:40
@LinInfoSec	Tensorflow - CVE-2022-29210: github.com/tensorflow/ten…	2022-05-21 06:00:52
/r/netcve	CVE-2022-29210	2022-05-21 00:38:13

← Previous ID

Next ID→

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