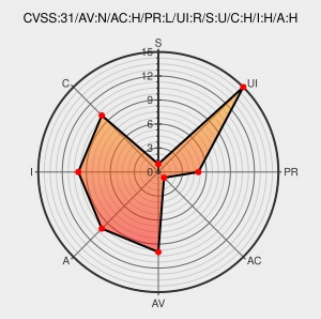
CVE-2022-41900

Published on: Not Yet Published

Last Modified on: 11/23/2022 01:35:00 PM UTC

CVE-2022-41900 - advisory for GHSA-xvwp-h6jv-7472

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. The security vulnerability results in FractionalMax(AVG)Pool with illegal pooling_ratio. Attackers using Tensorflow can exploit the vulnerability. They can access heap memory which is not in the control of user, leading to a crash or remote code execution. We have patched the issue in GitHub commit 216525144ee7c910296f5b05d214ca1327c9ce48. The fix will be included in TensorFlow 2.11.0. We will also cherry pick this commit on TensorFlow 2.10.1.

CVE-2022-41900 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.10.0, < 2.10.1**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.9.0, < 2.9.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 2.8.4**

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
Fix security vulnerability with FractionalMax(AVG)Pool with illegal p… · tensorflow/tensorflow@2165251	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/216525144ee7c910296f5b05d214ca1327c9ce48

· GitHub

FractionalMaxPool and FractionalAvgPool heap out-of-buffer · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-xvwp-h6jv-7472

Related QID Numbers

904596 Common Base Linux Mariner (CBL-Mariner) Security Update for tensorflow (11539)

904667 Common Base Linux Mariner (CBL-Mariner) Security Update for tensorflow (11539-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.10.0	All	All	All

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

cpe:2.3:a:google:tensorflow:2.10.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
/r/netcve	CVE-2022-41900	2022-11-18 22:38:35

← Previous ID

Next ID→