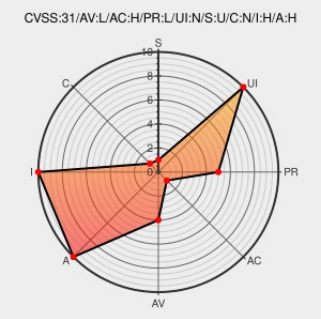
CVE-2021-29613

Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 10/25/2022 11:38:00 PM UTC

CVE-2021-29613 - advisory for GHSA-vvg4-vgrv-xfr7

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Tensorflow from Google contain the following vulnerability:

TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `tf.raw_ops.CTCLoss` allows an attacker to trigger an OOB read from heap. The fix will be included in TensorFlow 2.5.0. We will also cherrypick these commits on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE-2021-29613 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 2.1.4**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.2.0, < 2.2.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.3.0, < 2.3.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.4.0, < 2.4.2**

CVSS3 Score: 7.1 - HIGH

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

CVSS2 Score: 3.6 - LOW

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
Fix nullptr deref in `tf.raw_ops.CTCLoss`. · tensorflow/tensorflow@14607c0 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/14607c0707040d775e06b6817325640cb4b5864c
Fix OOB read issue with `tf.raw_ops.CTCLoss`. · tensorflow/tensorflow@4504a08 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/4504a081af71514bb1828048363e6540f797005b
Incomplete validation in `tf.raw_ops.CTCLoss` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-vvg4-vgrv-xfr7

Related QID Numbers

982442 Python (pip) Security Update for tensorflow-gpu (GHSA-vvg4-vgrv-xfr7)

Exploit/POC from Github

TensorFlow is an end-to-end open source platform for machine learning. Incomplete validation in `tf.raw_ops.CTCLoss` …

Known Affected Configurations (CPE V2.3)

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

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

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

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