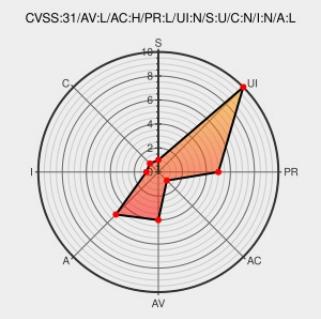
CVE-2021-29615

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

Last Modified on: 05/18/2021 06:22:00 PM UTC

CVE-2021-29615 - advisory for GHSA-qw5h-7f53-xrp6

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. The implementation of

`ParseAttrValue`(https://github.com/tensorflow/tensorflow/blob/c22d88d6ff33031aa113e48aa3fL453) can be tricked into stack overflow due to recursion by giving in a specially crafted input. The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit 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-2021-29615 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM 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: 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
Prevent memory overflow in ParseAttrValue from nested tensors. · tensorflow/tensorflow@e07e1c3 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/e07e1c3d26492c06f078c7e5bf2d138043e199c1
Stack overflow in `ParseAttrValue` with nested tensors · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-qw5h-7f53-xrp6

Related QID Numbers

982440 Python (pip) Security Update for tensorflow-gpu (GHSA-qw5h-7f53-xrp6)

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)
@CVEreport	CVE-2021-29615 : TensorFlow is an end-to-end open source platform for machine learning. The implementation of `Pars… twitter.com/i/web/status/1…	2021-05-14 20:06:44

← Previous ID

Next ID→

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