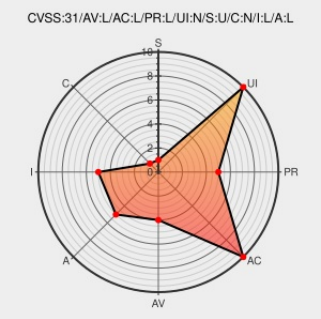
CVE-2020-26270

Published on: 12/10/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:56 PM UTC

CVE-2020-26270 - advisory for GHSA-m648-33qf-v3gp

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



Certain versions of Tensorflow from Google contain the following vulnerability:

In affected versions of TensorFlow running an LSTM/GRU model where the LSTM/GRU layer receives an input with zero-length results in a CHECK failure when using the CUDA backend. This can result in a query-of-death vulnerability, via denial of service, if users can control the input to the layer. This is fixed in versions 1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, and 2.4.0.

CVE-2020-26270 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as LOW severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 1.15.5**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.0.0, < 2.0.4**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.1.0, < 2.1.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.2.0, < 2.2.2**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.3.0, < 2.3.2**

CVSS3 Score: 3.3 - LOW

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

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
CHECK-fail in LSTM with zero-length input · Advisory · tensorflow/tensorflow · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-m648-33qf-v3gp
Prevent CHECK-fail in LSTM/GRU with zero-length input. · tensorflow/tensorflow@1475541 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/tensorflow/tensorflow/commit/14755416e364f17fb1870882fa778c7fec7f1

Related QID Numbers

983230 Python (pip) Security Update for tensorflow-gpu (GHSA-m648-33qf-v3gp)

Known Affected Configurations (CPE V2.3)

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

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→