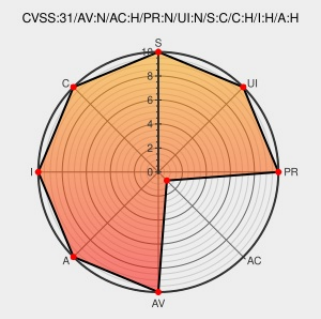
CVE-2020-15206

Published on: 09/25/2020 12:00:00 AM UTC

Last Modified on: 09/16/2021 03:45:00 PM UTC

CVE-2020-15206 - advisory for GHSA-w5gh-2wr2-pm6g

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



Certain versions of Tensorflow from Google contain the following vulnerability:

In Tensorflow before versions 1.15.4, 2.0.3, 2.1.2, 2.2.1 and 2.3.1, changing the TensorFlow's `SavedModel` protocol buffer and altering the name of required keys results in segfaults and data corruption while loading the model. This can cause a denial of service in products using `tensorflow-serving` or other inference-as-a-service installments. Fixed were added in commits f760f88b4267d981e13f4b302c437ae800445968 and fcfef195637c6e365577829c4d67681695956e7d (both going into TensorFlow 2.2.0 and 2.3.0 but not yet backported to earlier versions). However, this was not enough, as #41097 reports a different failure mode. The issue is patched in commit adf095206f25471e864a8e63a0f1caef53a0e3a6, and is released in TensorFlow versions 1.15.4, 2.0.3, 2.1.2, 2.2.1, or 2.3.1.

CVE-2020-15206 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 1.15.4**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.0.0, < 2.0.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.1.0, < 2.1.2**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.2.0, < 2.2.1**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.3.0, < 2.3.1**

CVSS3 Score: 7.5 - HIGH

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Validate `NodeDef`s from `FunctionDefLibrary` of a `GraphDef`. · tensorflow/tensorflow@adf0952 · GitHub	Patch, Third Party Advisory, Vendor Advisory, github.com, text/html	MISC github.com/tensorflow/tensorflow/commit/adf095206f25471e864a8e63a0f1caef53a0e
Incomplete validation in TensorFlow's SavedModel's constant nodes causes segfaults · Advisory · tensorflow/tensorflow · GitHub	Exploit, Third Party Advisory, github.com, text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-w5gh-2wr2-pm6g
Release TensorFlow 2.3.1 · tensorflow/tensorflow · GitHub	Third Party Advisory, github.com, text/html	MISC github.com/tensorflow/tensorflow/releases/tag/v2.3.1
[security-announce] openSUSE-SU-2020:1766-1: moderate: Security update f	lists.opensuse.org, text/html	SUSE openSUSE-SU-2020:1766

Related QID Numbers

981467 Python (pip) Security Update for tensorflow-gpu (GHSA-w5gh-2wr2-pm6g)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All
Application	Tensorflow	Tensorflow	All	All	All	All
Application	Tensorflow	Tensorflow	All	All	All	All

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

cpe:2.3:o:opensuse:leap:15.2:*:*:*:*:*:*:*:

cpe:2.3:a:tensorflow:tensorflow:*:*:*:*:-:*:*:*:

cpe:2.3:a:tensorflow:tensorflow:*:*:*:*:-:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Tensorflow - CVE-2020-15206: github.com/tensorflow/ten…	2021-09-16 19:45:19

← Previous ID

Next ID→