Incomplete validation in TensorFlow's SavedModel's constant nodes causes segfaults

Critical mihaimaruseac published GHSA-w5gh-2wr2-pm6g on Sep 24, 2020

Package

tensorflow, tensorflow-cpu, tensorflow-gpu (tensorflow)

Affected versions	Patched versions
< 2.3.0	1.15.4, 2.0.3, 2.1.2, 2.2.1, 2.3.1

Description

Impact

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.

We have added fixes to this in `f760f88` and `fcfef19` (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.

Patches

We have patched the issue in `adf0952` and will release patch releases for all versions between 1.15 and 2.3. Patch releases for versions between 1.15 and 2.1 will also contain cherry-picks of `f760f88` and `fcfef19` .

We recommend users to upgrade to TensorFlow 1.15.4, 2.0.3, 2.1.2, 2.2.1, or 2.3.1.

For more information

Please consult our security guide for more information regarding the security model and how to contact us with issues and questions.

Attribution

This vulnerability has been reported by Shuaike Dong, from Alipay Tian Qian Security Lab && Lab for Applied Security Research, CUHK.

Severity

Critical

CVE ID

CVE-2020-15206

Weaknesses

No CWEs