Segmentation fault and/or data corruption due to invalid TFLite model

Moderate **mihaimaruseac** published **GHSA-x9j7-x98r-r4w2** on Sep 24, 2020

Package

tensorflow-lite (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

If a TFLite saved model uses the same tensor as both input and output of an operator, then, depending on the operator, we can observe a segmentation fault or just memory corruption.

Patches

We have patched the issue in `d58c969` and will release patch releases for all versions between 1.15 and 2.3.

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

Workarounds

A potential workaround would be to add a custom `Verifier` to the model loading code to ensure that no operator reuses tensors as both inputs and outputs. Care should be taken to check all types of inputs (i.e., constant or variable tensors as well as optional tensors).

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 discovered from a variant analysis of GHSA-cvpc-8phh-8f45.

Severity

Moderate

CVE ID

CVE-2020-15210

Weaknesses

No CWEs