Null pointer dereference in TFLite

Moderate **mihaimaruseac** published **GHSA-qh32-6jjc-qprm** 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

A crafted TFLite model can force a node to have as input a tensor backed by a `nullptr` buffer. This can be achieved by changing a buffer index in the flatbuffer serialization to convert a read-only tensor to a read-write one. The runtime assumes that these buffers are written to before a possible read, hence they are initialized with `nullptr`:

tensorflow/tensorflow/lite/core/subgraph.cc
Lines 1224 to 1227 in `0e68f4d`

```
1224    TfLiteTensorReset(type, name, ConvertArrayToTfLiteIntArray(rank, dims),
1225                      GetLegacyQuantization(quantization),
1226                      /*buffer=*/nullptr, required_bytes, allocation_type,
1227                      nullptr, is_variable, &tensor);
```

However, by changing the buffer index for a tensor and implicitly converting that tensor to be a read-write one, as there is nothing in the model that writes to it, we get a null pointer dereference.

Patches

We have patched the issue in `0b5662b` 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.

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 members of the Aivul Team from Qihoo 360 but was also discovered through variant analysis of GHSA-cvpc-8phh-8f45.

Severity

Moderate

CVE ID

CVE-2020-15209

Weaknesses

No CWEs