Null pointer dereference in TFLite's `Reshape` operator

Moderate **mihaimaruseac** published **GHSA-jjr8-m8g8-p6wv** on May 12, 2021

Package

tensorflow-lite (pip)

Affected versions	Patched versions
< 2.5.0	2.1.4, 2.2.3, 2.3.3, 2.4.2

Description

Impact

The fix for CVE-2020-15209 missed the case when the target shape of `Reshape` operator is given by the elements of a 1-D tensor. As such, the fix for the vulnerability allowed passing a null-buffer-backed tensor with a 1D shape:

```
if (tensor->data.raw == nullptr && tensor->bytes > 0) {
  if (registration.builtin_code == kTfLiteBuiltinReshape && i == 1) {
    // In general, having a tensor here with no buffer will be an error.
    // However, for the reshape operator, the second input tensor is only
    // used for the shape, not for the data. Thus, null buffer is ok.
    continue;
  } else {
    // In all other cases, we need to return an error as otherwise we will
    // trigger a null pointer dereference (likely).
    ReportError("Input tensor %d lacks data", tensor_index);
    return kTfLiteError;
  }
}
```

Patches

We have patched the issue in GitHub commit f8378920345f4f4604202d4ab15ef64b2aceaa16.

The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

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.

Severity

Moderate

CVE ID

CVE-2021-29592

Weaknesses

No CWEs