Division by zero in TFLite's implementation of `OneHot`

Low mihaimaruseac published GHSA-j8qh-3xrq-c825 on May 12, 2021

Package

tensorflow-lite (pip)

Affected versions

< 2.5.0

Patched versions

2.1.4, 2.2.3, 2.3.3, 2.4.2

Description

Impact

The implementation of the `OneHot` TFLite operator is vulnerable to a division by zero error:

```
int prefix_dim_size = 1;
for (int i = 0; i < op_context.axis; ++i) {
  prefix_dim_size *= op_context.indices->dims->data[i];
}
const int suffix_dim_size = NumElements(op_context.indices) / prefix_dim_size;
```

An attacker can craft a model such that at least one of the dimensions of `indices` would be 0. In turn, the `prefix_dim_size` value would become 0.

Patches

We have patched the issue in GitHub commit 3ebedd7e345453d68e279cfc3e4072648e5e12e5.

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

Low

CVE ID

CVE-2021-29600

Weaknesses

No CWEs