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

Low **mihaimaruseac** published **GHSA-rf3h-xgv5-2q39** 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 implementation of the `DepthwiseConv` TFLite operator is vulnerable to a division by zero error:

```
int num_input_channels = SizeOfDimension(input, 3);
TF_LITE_ENSURE_EQ(context, num_filter_channels % num_input_channels, 0);
```

An attacker can craft a model such that `input`'s fourth dimension would be 0.

Patches

We have patched the issue in GitHub commit cbda3c6b2dbbd3fbdc482ff8c0170a78ec2e97d0.

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-2021-29602

Weaknesses

No CWEs