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

Low **mihaimaruseac** published **GHSA-4vrf-ff7v-hpgr** 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

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

```
const int row_size = SizeOfDimension(value, 0);
const int row_bytes = value->bytes / row_size;
```

An attacker can craft a model such that the first dimension of the `value` input is 0.

Patches

We have patched the issue in GitHub commit f61c57bd425878be108ec787f4d96390579fb83e.

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-2021-29596

Weaknesses

No CWEs