Division by zero in TFLite's implementation of hashtable lookup

Low **mihaimaruseac** published **GHSA-8rm6-75mf-7r7r** 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 TFLite implementation of hashtable lookup is vulnerable to a division by zero error:

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

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

Patches

We have patched the issue in GitHub commit 5117e0851348065ed59c991562c0ec80d9193db2.

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-2021-29604

Weaknesses

No CWEs