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

Low **mihaimaruseac** published **GHSA-3w67-q784-6w7c** 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 reference implementation of the `GatherNd` TFLite operator is vulnerable to a division by zero error:

```
ret.dims_to_count[i] = remain_flat_size / params_shape.Dims(i);
```

An attacker can craft a model such that `params` input would be an empty tensor. In turn, `params_shape.Dims(.)` would be zero, in at least one dimension.

Patches

We have patched the issue in GitHub commit 8e45822aa0b9f5df4b4c64f221e64dc930a70a9d.

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-2021-29589

Weaknesses

No CWEs