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

Low mihaimaruseac published **GHSA-j7rm-8ww4-xx2g** 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 `Prepare` step of the `SpaceToDepth` TFLite operator does not check for 0 before division.

```
  const int block_size = params->block_size;
  const int input_height = input->dims->data[1];
  const int input_width = input->dims->data[2];
  int output_height = input_height / block_size;
  int output_width = input_width / block_size;
```

An attacker can craft a model such that `params->block_size` would be zero.

Patches

We have patched the issue in GitHub commit [0d45ea1ca641b21b73bcf9c00e0179cda284e7e7](0d45ea1ca641b21b73bcf9c00e0179cda284e7e7).

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-2021-29587

Weaknesses

No CWEs