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

Low **mihaimaruseac** published **GHSA-vf94-36g5-69v8** on May 12, 2021

Package

tensorflow, tensorflow-cpu, tensorflow-gpu (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 `DepthToSpace` TFLite operator is vulnerable to a division by zero error:

```
const int block_size = params->block_size;
...
const int input_channels = input->dims->data[3];
...
int output_channels = input_channels / block_size / block_size;
```

An attacker can craft a model such that `params->block_size` is 0.

Patches

We have patched the issue in GitHub commit 106d8f4fb89335a2c52d7c895b7a7485465ca8d9.

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-2021-29595

Weaknesses

No CWEs