


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

Low mihairmaruseac published GHSA-vfr4-x8j2-3rf9 on May 12, 2021

Package

 tensorflow-lite (pip)

Affected versions

< 2.5.0

Patched versions

2.1.4, 2.2.3, 2.3.3, 2.4.2

Description

Impact

The optimized implementation of the `TransposeConv` TFLite operator is [vulnerable to a division by zero error](#):

```
int height_col = (height + pad_t + pad_b - filter_h) / stride_h + 1;
int width_col = (width + pad_l + pad_r - filter_w) / stride_w + 1;
```

An attacker can craft a model such that `stride_{h,w}` values are 0. Code calling this function must validate these arguments.

Patches

We have patched the issue in GitHub commit [801c1c6be5324219689c98e1bd3e0ca365ee834d](#).

The fix will be included in TensorFlow 2.5.0. We will also cherry-pick 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-2021-29588

Weaknesses

No CWEs