tensorflow / **tensorflow** Public

<> Code   ⊙ Issues 2.1k   ⟙ Pull requests 313   ▷ Actions   ⊞ Projects 2   ...

Division by zero in TFLite's convolution code

Low   **mihaimaruseac** published **GHSA-3qgw-p4fm-x7gf** 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

TFLite's convolution code has multiple division where the divisor is controlled by the user and not checked to be non-zero. For example:

```
const int input_size = NumElements(input) / SizeOfDimension(input, 0);
```

Patches

We have patched the issue in GitHub commit ff489d95a9006be080ad14feb378f2b4dac35552.

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-2021-29594

Weaknesses

No CWEs