Division by zero in optimized pooling implementations in TFLite

Low **mihaimaruseac** published **GHSA-26j7-6w8w-7922** 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

Optimized pooling implementations in TFLite fail to check that the stride arguments are not 0 before calling `ComputePaddingHeightWidth`.

Since users can craft special models which will have `params->stride_{height,width}` be zero, this will result in a division by zero.

Patches

We have patched the issue in GitHub commit 5f7975d09eac0f10ed8a17dbb6f5964977725adc.

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-2021-29586

Weaknesses

No CWEs