Stack overflow due to looping TFLite subgraph

High **mihaimaruseac** published **GHSA-cwv3-863g-39vx** 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 graphs must not have loops between nodes. However, this condition was not checked and an attacker could craft models that would result in infinite loop during evaluation. In certain cases, the infinite loop would be replaced by stack overflow due to too many recursive calls.

For example, the `While` implementation could be tricked into a scneario where both the body and the loop subgraphs are the same. Evaluating one of the subgraphs means calling the `Eval` function for the other and this quickly exhaust all stack space.

Patches

We have patched the issue in GitHub commit 9c1dc920d8ffb4893d6c9d27d1f039607b326743 (for the `While` operator) and in GitHub commit c6173f5fe66cdbab74f4f869311fe6aae2ba35f4 (in general).

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

High

CVE ID

CVE-2021-29591

Weaknesses

No CWEs