Integer overflow in TFLite concatentation

High **mihaimaruseac** published **GHSA-9c84-4hx6-xmm4** 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

The TFLite implementation of concatenation is vulnerable to an integer overflow issue:

```
for (int d = 0; d < t0->dims->size; ++d) {
  if (d == axis) {
    sum_axis += t->dims->data[axis];
  } else {
    TF_LITE_ENSURE_EQ(context, t->dims->data[d], t0->dims->data[d]);
  }
}
```

An attacker can craft a model such that the dimensions of one of the concatenation input overflow the values of `int`. TFLite uses `int` to represent tensor dimensions, whereas TF uses `int64`. Hence, valid TF models can trigger an integer overflow when converted to TFLite format.

Patches

We have patched the issue in GitHub commit 4253f96a58486ffe84b61c0415bb234a4632ee73.

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-2021-29601

Weaknesses

No CWEs