Integer overflow in TFLite memory allocation

Critical **mihaimaruseac** published **GHSA-jf7h-7m85-w2v2** 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 code for allocating `TFLiteIntArray` s is vulnerable to an integer overflow issue:

```
int TfLiteIntArrayGetSizeInBytes(int size) {
  static TfLiteIntArray dummy;
  return sizeof(dummy) + sizeof(dummy.data[0]) * size;
}
```

An attacker can craft a model such that the `size` multiplier is so large that the return value overflows the `int` datatype and becomes negative. In turn, this results in invalid value being given to `malloc` :

```
TfLiteIntArray* TfLiteIntArrayCreate(int size) {
  TfLiteIntArray* ret = (TfLiteIntArray*)malloc(TfLiteIntArrayGetSizeInBytes(size));
  ret->size = size;
  return ret;
}
```

In this case, `ret->size` would dereference an invalid pointer.

Patches

We have patched the issue in GitHub commit 7c8cc4ec69cd348e44ad6a2699057ca88faad3e5.

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

Critical

CVE ID

CVE-2021-29605

Weaknesses

No CWEs