Heap OOB write in TFLite

Moderate **mihaimaruseac** published **GHSA-crch-j389-5f84** 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

A specially crafted TFLite model could trigger an OOB write on heap in the TFLite implementation of `ArgMin` / `ArgMax` :

```
TfLiteIntArray* output_dims = TfLiteIntArrayCreate(NumDimensions(input) - 1);
int j = 0;
for (int i = 0; i < NumDimensions(input); ++i) {
  if (i != axis_value) {
    output_dims->data[j] = SizeOfDimension(input, i);
    ++j;
  }
}
```

If `axis_value` is not a value between 0 and `NumDimensions(input)` , then the condition in the `if` is never true, so code writes past the last valid element of `output_dims->data` .

Patches

We have patched the issue in GitHub commit c59c37e7b2d563967da813fa50fe20b21f4da683.

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

Moderate

CVE ID

CVE-2021-29603

Weaknesses

No CWEs