Heap OOB read in TFLite's implementation of `Minimum` or `Maximum`

Low mihaimaruseac published GHSA-24x6-8c7m-hv3f on May 12, 2021

Package

tensorflow-lite (pip)

Affected versions

< 2.5.0

Patched versions

2.1.4, 2.2.3, 2.3.3, 2.4.2

Description

Impact

The implementations of the `Minimum` and `Maximum` TFLite operators can be used to read data outside of bounds of heap allocated objects, if any of the two input tensor arguments are empty.

This is because the broadcasting implementation indexes in both tensors with the same index but does not validate that the index is within bounds:

```
auto maxmin_func = [&](int indexes[N]) {
  output_data[SubscriptToIndex(output_desc, indexes)] =
    op(input1_data[SubscriptToIndex(desc1, indexes)],
       input2_data[SubscriptToIndex(desc2, indexes)]);
};
```

Patches

We have patched the issue in GitHub commit 953f28dca13c92839ba389c055587cfe6c723578.

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-2021-29590

Weaknesses

No CWEs