Denial of service from TFLite implementation of segment sum

Moderate **mihaimaruseac** published **GHSA-hjmq-236j-8m87** on Sep 24, 2020

Package

tensorflow-lite (tensorflow)

Affected versions

2.2.0, 2.3.0

Patched versions

2.2.1, 2.3.1

Description

Impact

In TensorFlow Lite models using segment sum can trigger a denial of service by causing an out of memory allocation in the implementation of segment sum. Since code uses the last element of the tensor holding them to determine the dimensionality of output tensor, attackers can use a very large value to trigger a large allocation:

tensorflow/tensorflow/lite/kernels/segment_sum.cc
Lines 39 to 44 in 0e68f4d

```
39      if (segment_id_size > 0) {
40        max_index = segment_ids->data.i32[segment_id_size - 1];
41      }
42      const int data_rank = NumDimensions(data);
43      TfLiteIntArray* output_shape = TfLiteIntArrayCreate(NumDimensions(data));
44      output_shape->data[0] = max_index + 1;
```

Patches

We have patched the issue in `204945b` and will release patch releases for all affected versions.

We recommend users to upgrade to TensorFlow 2.2.1, or 2.3.1.

Workarounds

A potential workaround would be to add a custom `Verifier` to limit the maximum value in the segment ids tensor. This only handles the case when the segment ids are stored statically in the model, but a similar validation could be done if the segment ids are generated at runtime, between inference steps.

However, if the segment ids are generated as outputs of a tensor during inference steps, then there are no possible workaround and users are advised to upgrade to patched code.

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 discovered from a variant analysis of GHSA-p2cq-cprg-frvm.

Severity

Moderate

CVE ID

CVE-2020-15213

Weaknesses

No CWEs