Heap OOB read in TFLite

High **mihaimaruseac** published **GHSA-h4pc-gx2w-f2xv** 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 read on heap in the TFLite implementation of `Split_V`:

```
const int input_size = SizeOfDimension(input, axis_value);
```

If `axis_value` is not a value between 0 and `NumDimensions(input)`, then the `SizeOfDimension` function will access data outside the bounds of the tensor shape array:

```
inline int SizeOfDimension(const TfLiteTensor* t, int dim) {
  return t->dims->data[dim];
}
```

Patches

We have patched the issue in GitHub commit ae2daeb45abfe2c6dda539cf8d0d6f653d3ef412.

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-2021-29606

Weaknesses

No CWEs