Heap buffer overflow due to invalid splits in RaggedCountSparseOutput

Moderate **mihaimaruseac** published **GHSA-p5f8-gfw5-33w4** on Sep 24, 2020

Package

tensorflow, tensorflow-cpu, tensorflow-gpu (tensorflow)

Affected versions	Patched versions
2.3.0	2.3.1

Description

Impact

The `RaggedCountSparseOutput` implementation does not validate that the input arguments form a valid ragged tensor. In particular, there is no validation that the values in the `splits` tensor generate a valid partitioning of the `values` tensor. Hence, this code is prone to heap buffer overflow:

tensorflow/tensorflow/core/kernels/count_ops.cc
Lines 248 to 251 in `0e68f4d`

```
248      for (int idx = 0; idx < num_values; ++idx) {
249        while (idx >= splits_values(batch_idx)) {
250          batch_idx++;
251        }
```

If `split_values` does not end with a value at least `num_values` then the `while` loop condition will trigger a read outside of the bounds of `split_values` once `batch_idx` grows too large.

Patches

We have patched the issue in `3cbb917` and will release a patch release.

We recommend users to upgrade to TensorFlow 2.3.1.

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-2020-15201

Weaknesses

No CWEs