Heap buffer overflow due to invalid indices in SparseCountSparseOutput

Moderate **mihaimaruseac** published **GHSA-jc87-6vpp-7ff3** on Sep 24, 2020

Package

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

Affected versions	Patched versions
2.3.0	2.3.1

Description

Impact

The `SparseCountSparseOutput` implementation does not validate that the input arguments form a valid sparse tensor. In particular, there is no validation that the `indices` tensor has the same shape as the `values` one. The values in these tensors are always accessed in parallel:

tensorflow/tensorflow/core/kernels/count_ops.cc
Lines 193 to 195 in `0e68f4d`

```
193     for (int idx = 0; idx < num_values; ++idx) {
194       int batch = is_1d ? 0 : indices_values(idx, 0);
195       const auto& value = values_values(idx);
```

Thus, a shape mismatch can result in accesses outside the bounds of heap allocated buffers.

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 is a variant of GHSA-p5f8-gfw5-33w4

Severity

Moderate

CVE ID

CVE-2020-15198

Weaknesses

No CWEs