Crash due to invalid splits in SparseCountSparseOutput

Moderate **mihaimaruseac** published **GHSA-qc53-44cj-vfvx** 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 rank 2. This tensor must be a matrix because code assumes its elements are accessed as elements of a matrix:

tensorflow/tensorflow/core/kernels/count_ops.cc
Line 185 in `0e68f4d`

```
185     const auto indices_values = indices.matrix<int64>();
```

However, malicious users can pass in tensors of different rank, resulting in a `CHECK` assertion failure and a crash. This can be used to cause denial of service in serving installations, if users are allowed to control the components of the input sparse tensor.

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-2020-15197

Weaknesses

No CWEs