Division by 0 in `Reverse`

Low **mihaimaruseac** published **GHSA-fxqh-cfjm-fp93** 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.Reverse`:

```
import tensorflow as tf

tensor_input = tf.constant([], shape=[0, 1, 1], dtype=tf.int32)
dims = tf.constant([False, True, False], shape=[3], dtype=tf.bool)

tf.raw_ops.Reverse(tensor=tensor_input, dims=dims)
```

This is because the implementation performs a division based on the first dimension of the tensor argument:

```
const int64 N = input.dim_size(0);
const int64 cost_per_unit = input.NumElements() / N;
```

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

Patches

We have patched the issue in GitHub commit 4071d8e2f6c45c1955a811fee757ca2adbe462c1.

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-2021-29556

Weaknesses

No CWEs