Overflow/denial of service in `tf.raw_ops.ReverseSequence`

Low **mihaimaruseac** published **GHSA-6qgm-fv6v-rfpv** 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

The implementation of `tf.raw_ops.ReverseSequence` allows for stack overflow and/or `CHECK` -fail based denial of service.

```
import tensorflow as tf

input = tf.zeros([1, 1, 1], dtype=tf.int32)
seq_lengths = tf.constant([0], shape=[1], dtype=tf.int32)

tf.raw_ops.ReverseSequence(
    input=input, seq_lengths=seq_lengths, seq_dim=-2, batch_dim=0)
```

The implementation fails to validate that `seq_dim` and `batch_dim` arguments are valid.

Negative values for `seq_dim` can result in stack overflow or `CHECK` -failure, depending on the version of Eigen code used to implement the operation. Similar behavior can be exhibited by invalid values of `batch_dim` .

Patches

We have patched the issue in GitHub commit ecf768cbe50cedc0a45ce1ee223146a3d3d26d23.

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-2021-29575

Weaknesses

No CWEs