Lack of validation in `SparseDenseCwiseMul`

Low **mihaimaruseac** published **GHSA-wp3c-xw9g-gpcg** 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

Due to lack of validation in `tf.raw_ops.SparseDenseCwiseMul`, an attacker can trigger denial of service via `CHECK`-fails or accesses to outside the bounds of heap allocated data:

```
import tensorflow as tf

indices = tf.constant([], shape=[10, 0], dtype=tf.int64)
values = tf.constant([], shape=[0], dtype=tf.int64)
shape = tf.constant([0, 0], shape=[2], dtype=tf.int64)
dense = tf.constant([], shape=[0], dtype=tf.int64)

tf.raw_ops.SparseDenseCwiseMul(
    sp_indices=indices, sp_values=values, sp_shape=shape, dense=dense)
```

Since the implementation only validates the rank of the input arguments but no constraints between dimensions, an attacker can abuse them to trigger internal `CHECK` assertions (and cause program termination, denial of service) or to write to memory outside of bounds of heap allocated tensor buffers.

Patches

We have patched the issue in GitHub commit 7ae2af34087fb4b5c8915279efd03da3b81028bc.

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 Yakun Zhang and Ying Wang of Baidu X-Team.

Severity

Low

CVE ID

CVE-2021-29567

Weaknesses

No CWEs