Heap out of bounds read in `RequantizationRange`

Low **mihaimaruseac** published **GHSA-3h8m-483j-7xxm** 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

The implementation of `tf.raw_ops.MaxPoolGradWithArgmax` can cause reads outside of bounds of heap allocated data if attacker supplies specially crafted inputs:

```
import tensorflow as tf

input = tf.constant([1], shape=[1], dtype=tf.qint32)
input_max = tf.constant([], dtype=tf.float32)
input_min = tf.constant([], dtype=tf.float32)

tf.raw_ops.RequantizationRange(input=input, input_min=input_min, input_max=input_max)
```

The implementation assumes that the `input_min` and `input_max` tensors have at least one element, as it accesses the first element in two arrays:

```
const float input_min_float = ctx->input(1).flat<float>()(0);
const float input_max_float = ctx->input(2).flat<float>()(0);
```

If the tensors are empty, `.flat<T>()` is an empty object, backed by an empty array. Hence, accesing even the 0th element is a read outside the bounds.

Patches

We have patched the issue in GitHub commit ef0c008ee84bad91ec6725ddc42091e19a30cf0e.

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 Ying Wang and Yakun Zhang of Baidu X-Team.

Severity

Low

CVE ID

CVE-2021-29569

Weaknesses

No CWEs