Heap OOB in `QuantizeAndDequantizeV3`

Low **mihaimaruseac** published **GHSA-h9px-9vqg-222h** 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 read data outside of bounds of heap allocated buffer in `tf.raw_ops.QuantizeAndDequantizeV3`:

```
import tensorflow as tf

tf.raw_ops.QuantizeAndDequantizeV3(
  input=[2.5,2.5], input_min=[0,0], input_max=[1,1], num_bits=[30],
  signed_input=False, range_given=False, narrow_range=False, axis=3)
```

This is because the implementation does not validate the value of user supplied `axis` attribute before using it to index in the array backing the `input` argument:

```
const int depth = (axis_ == -1) ? 1 : input.dim_size(axis_);
```

Patches

We have patched the issue in GitHub commit 99085e8ff02c3763a0ec2263e44daec416f6a387.

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 Aivul Team from Qihoo 360.

Severity

Low

CVE ID

CVE-2021-29553

Weaknesses

No CWEs