Segfault in `tf.quantization.quantize_and_dequantize`

Moderate **mihaimaruseac** published **GHSA-rrfp-j2mp-hq9c** on Oct 20, 2020

Package

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

Affected versions	Patched versions
< 2.4.0	2.4.0

Description

Impact

An attacker can pass an invalid `axis` value to `tf.quantization.quantize_and_dequantize`:

```
tf.quantization.quantize_and_dequantize(
    input=[2.5, 2.5], input_min=[0,0], input_max=[1,1], axis=10)
```

This results in accessing a dimension outside the rank of the input tensor in the C++ kernel implementation:

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

However, `dim_size` only does a `DCHECK` to validate the argument and then uses it to access the corresponding element of an array:

```
int64 TensorShapeBase<Shape>::dim_size(int d) const {
  DCHECK_GE(d, 0);
  DCHECK_LT(d, dims());
  DoStuffWith(dims_[d]);
}
```

Since in normal builds, `DCHECK`-like macros are no-ops, this results in segfault and access out of bounds of the array.

Patches

We have patched the issue in `eccb7ec` and will release TensorFlow 2.4.0 containing the patch. TensorFlow nightly packages after this commit will also have the issue resolved.

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 in #42105

Severity

Moderate

CVE ID

CVE-2020-15265

Weaknesses

No CWEs