Segfault due to missing support for quantized types

Low mihaimaruseac published GHSA-54ch-gjq5-4976 on May 17

Package

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

Affected versions

< 2.9.0

Patched versions

2.6.4, 2.7.2, 2.8.1, 2.9.0

Description

Impact

There is a potential for segfault / denial of service in TensorFlow by calling `tf.compat.v1.*` ops which don't yet have support for quantized types (added after migration to TF 2.x):

```
import numpy as np
import tensorflow as tf

tf.compat.v1.placeholder_with_default(input=np.array([2]),shape=tf.constant(dtype=tf.qint8, valu
```

In these scenarios, since the kernel is missing, a `nullptr` value is passed to `ParseDimensionValue` for the `py_value` argument. Then, this is dereferenced, resulting in segfault.

Patches

We have patched the issue in GitHub commit 237822b59fc504dda2c564787f5d3ad9c4aa62d9.

The fix will be included in TensorFlow 2.9.0. We will also cherrypick this commit on TensorFlow 2.8.1, TensorFlow 2.7.2, and TensorFlow 2.6.4, 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 Hong Jin from Singapore Management University.

Severity

Low

CVE ID

CVE-2022-29205

Weaknesses

No CWEs