# Segfault if `tf.histogram_fixed_width` is called with NaN values

High mihaimaruseac published GHSA-xrp2-fhq4-4q3w on May 17

Package

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

| Affected versions | Patched versions |
|---|---|
| < 2.9.0 | 2.6.4, 2.7.2, 2.8.1, 2.9.0 |

## Description

### Impact

The implementation of `tf.histogram_fixed_width` is vulnerable to a crash when the values array contain `NaN` elements:

```
import tensorflow as tf
import numpy as np

tf.histogram_fixed_width(values=np.nan, value_range=[1,2])
```

The implementation assumes that all floating point operations are defined and then converts a floating point result to an integer index:

```
index_to_bin.device(d) =
    ((values.cwiseMax(value_range(0)) - values.constant(value_range(0)))
         .template cast<double>() /
     step)
        .cwiseMin(nbins_minus_1)
        .template cast<int32>();
```

If `values` contains `NaN` then the result of the division is still `NaN` and the cast to `int32` would result in a crash.

This only occurs on the CPU implementation.

### Patches

We have patched the issue in GitHub commit e57fd691c7b0fd00ea3bfe43444f30c1969748b5.

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 externally via a GitHub issue.

**Severity**

High

**CVE ID**

CVE-2022-29211

**Weaknesses**

No CWEs