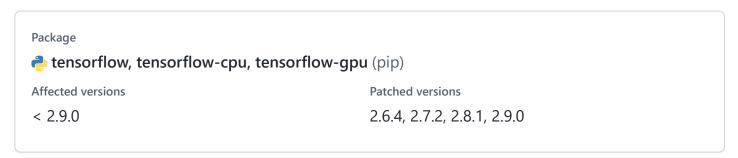


# Undefined behavior when users supply invalid resource handles

(Low)

mihaimaruseac published GHSA-5wpj-c6f7-24x8 on May 17



#### Description

## **Impact**

Multiple TensorFlow operations misbehave in eager mode when the resource handle provided to them is invalid:

```
import tensorflow as tf

tf.raw_ops.QueueIsClosedV2(handle=[])

import tensorflow as tf

tf.summary.flush(writer=())
```

In graph mode, it would have been impossible to perform these API calls, but migration to TF 2.x eager mode opened up this vulnerability. If the resource handle is empty, then a reference is bound to a null pointer inside TensorFlow codebase (various codepaths). This is undefined behavior.

## **Patches**

We have patched the issue in GitHub commit a5b89cd68c02329d793356bda85d079e9e69b4e7 and GitHub commit dbdd98c37bc25249e8f288bd30d01e118a7b4498.

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

 $(\mathsf{Low})$ 

**CVE ID** 

CVE-2022-29207

#### Weaknesses

No CWEs