Missing validation causes `TensorSummaryV2` to crash

Low   mihaimaruseac published **GHSA-2p9q-h29j-3f5v** 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.raw_ops.TensorSummaryV2` does not fully validate the input arguments. This results in a `CHECK`-failure which can be used to trigger a denial of service attack:

```python
import numpy as np
import tensorflow as tf

tf.raw_ops.TensorSummaryV2(
    tag=np.array('test'),
    tensor=np.array(3),
    serialized_summary_metadata=tf.io.encode_base64(np.empty((0))))
```

The code assumes `axis` is a scalar but there is no validation for this.

```cpp
const Tensor& serialized_summary_metadata_tensor = c->input(2);
// ...
ParseFromTString(serialized_summary_metadata_tensor.scalar<tstring>()(),
                 v->mutable_metadata());
```

Patches

We have patched the issue in GitHub commit 290bb05c80c327ed74fae1d089f1001b1e2a4ef7.

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 Neophytos Christou from Secure Systems Lab at Brown University and Hong Jin from Singapore Management University.

Severity

Low

CVE ID

CVE-2022-29193

Weaknesses

No CWEs