Missing validation causes denial of service via `DeleteSessionTensor`

Low   **mihaimaruseac** published **GHSA-h5g4-ppwx-48q2** 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.DeleteSessionTensor` 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 tensorflow as tf

handle = tf.constant("[]", shape=[0], dtype=tf.string)
tf.raw_ops.DeleteSessionTensor(handle=handle)
```

The code assumes `handle` is a scalar but there is no validation for this:

```cpp
    const Tensor& handle = ctx->input(0);
    const string& name = handle.scalar<tstring>()();
```

Patches

We have patched the issue in GitHub commit cff267650c6a1b266e4b4500f69fbc49cdd773c5.

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.

Severity

Low

CVE ID

CVE-2022-29194

Weaknesses

No CWEs