

Missing validation causes denial of service via `GetSessionTensor`

Low mihairmaruseac published GHSA-fv25-wrff-wf86 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

The implementation of `tf.raw_ops.GetSessionTensor` does not fully validate the input arguments. This results in a `CHECK`-failure which can be used to trigger a denial of service attack:

```
import tensorflow as tf

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

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

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

Patches

We have patched the issue in GitHub commit [48305e8ffe5246d67570b64096a96f8e315a7281](https://github.com/tensorflow/tensorflow/commit/48305e8ffe5246d67570b64096a96f8e315a7281).

The fix will be included in TensorFlow 2.9.0. We will also cherry-pick 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-2022-29191

Weaknesses

No CWEs