

Denial of service in `tf.ragged.constant` due to lack of validation

Low mihairmaruseac published GHSA-cwpm-f78v-7m5c 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.ragged.constant` does not fully validate the input arguments. This results in a denial of service by consuming all available memory:

```
import tensorflow as tf
tf.ragged.constant(pylist=[], ragged_rank=8968073515812833920)
```

Patches

We have patched the issue in GitHub commit [bd4d5583ff9c8df26d47a23e508208844297310e](#).

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

Low

CVE ID

CVE-2022-29202

Weaknesses

No CWEs