Crash in `tf.strings.substr` due to `CHECK`-fail

Low **mihaimaruseac** published **GHSA-mmq6-q8r3-48fm** on May 12, 2021

Package

🐍 **tensorflow, tensorflow-cpu, tensorflow-gpu** (pip)

Affected versions   **Patched versions**

< 2.5.0   2.1.4, 2.2.3, 2.3.3, 2.4.2

Description

Impact

An attacker can cause a denial of service via `CHECK`-fail in `tf.strings.substr` with invalid arguments:

```
import tensorflow as tf
tf.strings.substr(input='abc', len=1, pos=[1,-1])
```

```
import tensorflow as tf
tf.strings.substr(input='abc', len=1, pos=[1,2])
```

Patches

We have received a patch for the issue in GitHub commit 890f7164b70354c57d40eda52dcdd7658677c09f.

The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, 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 in #46900 and fixed in #46974.

Severity

Low

CVE ID

CVE-2021-29617

Weaknesses

No CWEs