Reference binding to null in `ParameterizedTruncatedNormal`

Low **mihaimaruseac** published **GHSA-4p4p-www8-8fv9** 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 undefined behavior by binding to null pointer in `tf.raw_ops.ParameterizedTruncatedNormal`:

```
import tensorflow as tf

shape = tf.constant([], shape=[0], dtype=tf.int32)
means = tf.constant((1), dtype=tf.float32)
stdevs = tf.constant((1), dtype=tf.float32)
minvals = tf.constant((1), dtype=tf.float32)
maxvals = tf.constant((1), dtype=tf.float32)

tf.raw_ops.ParameterizedTruncatedNormal(
  shape=shape, means=means, stdevs=stdevs, minvals=minvals, maxvals=maxvals)
```

This is because the implementation does not validate input arguments before accessing the first element of `shape`:

```
int32 num_batches = shape_tensor.flat<int32>()(0);
```

If `shape` argument is empty, then `shape_tensor.flat<T>()` is an empty array.

Patches

We have patched the issue in GitHub commit 5e52ef5a461570cfb68f3bdbbebfe972cb4e0fd8.

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 Ying Wang and Yakun Zhang of Baidu X-Team.

Severity

Low

CVE ID

CVE-2021-29568

Weaknesses

No CWEs