Reference binding to null pointer in `MatrixDiag*` ops

Low **mihaimaruseac** published **GHSA-hc6c-75p4-hmq4** 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 `MatrixDiag*` operations does not validate that the tensor arguments are non-empty:

```
      num_rows = context->input(2).flat<int32>()(0);
      num_cols = context->input(3).flat<int32>()(0);
      padding_value = context->input(4).flat<T>()(0);
```

Thus, users can trigger null pointer dereferences if any of the above tensors are null:

```
import tensorflow as tf

d = tf.convert_to_tensor([],dtype=tf.float32)
p = tf.convert_to_tensor([],dtype=tf.float32)
tf.raw_ops.MatrixDiagV2(diagonal=d, k=0, num_rows=0, num_cols=0, padding_value=p)
```

Changing from `tf.raw_ops.MatrixDiagV2` to `tf.raw_ops.MatrixDiagV3` still reproduces the issue.

Patches

We have patched the issue in GitHub commit a7116dd3913c4a4afd2a3a938573aa7c785fdfc6.

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 Ye Zhang and Yakun Zhang of Baidu X-Team.

Severity

Low

CVE ID

CVE-2021-29515

Weaknesses

No CWEs