# Missing validation results in undefined behavior in `SparseTensorDenseAdd

Low **mihaimaruseac** published **GHSA-rc9w-5c64-9vqq** on May 17

Package

**tensorflow, tensorflow-cpu, tensorflow-gpu** (pip)

| Affected versions | Patched versions |
| --- | --- |
| < 2.9.0 | 2.6.4, 2.7.2, 2.8.1, 2.9.0 |

## Description

### Impact

The implementation of `tf.raw_ops.SparseTensorDenseAdd` does not fully validate the input arguments:

```
import tensorflow as tf

a_indices = tf.constant(0, shape=[17, 2], dtype=tf.int64)
a_values = tf.constant([], shape=[0], dtype=tf.float32)
a_shape = tf.constant([6, 12], shape=[2], dtype=tf.int64)

b = tf.constant(-0.223668531, shape=[6, 12], dtype=tf.float32)

tf.raw_ops.SparseTensorDenseAdd(
    a_indices=a_indices, a_values=a_values, a_shape=a_shape, b=b)
```

In this case, a reference gets bound to a `nullptr` during kernel execution. This is UB.

### Patches

We have patched the issue in GitHub commit 11ced8467eccad9c7cb94867708be8fa5c66c730.

The fix will be included in TensorFlow 2.9.0. We will also cherrypick this commit on TensorFlow 2.8.1, TensorFlow 2.7.2, and TensorFlow 2.6.4, 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 Neophytos Christou from Secure Systems Lab at Brown University.

**Severity**

Low

**CVE ID**

CVE-2022-29206

**Weaknesses**

No CWEs