Heap buffer overflow in `SparseTensorToCSRSparseMatrix`

Low **mihaimaruseac** published **GHSA-hmg3-c7xj-6qwm** 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

An attacker can trigger a denial of service via a `CHECK` -fail in converting sparse tensors to CSR Sparse matrices:

```
import tensorflow as tf
import numpy as np
from tensorflow.python.ops.linalg.sparse import sparse_csr_matrix_ops

indices_array = np.array([[0, 0]])
value_array = np.array([0.0], dtype=np.float32)
dense_shape = [0, 0]

st = tf.SparseTensor(indices_array, value_array, dense_shape)

values_tensor = sparse_csr_matrix_ops.sparse_tensor_to_csr_sparse_matrix(
      st.indices, st.values, st.dense_shape)
```

This is because the implementation does a double redirection to access an element of an array allocated on the heap:

```
csr_row_ptr(indices(i, 0) + 1) += 1;
```

If the value at `indices(i, 0)` is such that `indices(i, 0) + 1` is outside the bounds of `csr_row_ptr` , this results in writing outside of bounds of heap allocated data.

Patches

We have patched the issue in GitHub commit 1e922ccdf6bf46a3a52641f99fd47d54c1decd13.

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

Low

CVE ID

CVE-2021-29545

Weaknesses

No CWEs