Heap buffer overflow in SparseFillEmptyRowsGrad

High **mihaimaruseac** published **GHSA-63xm-rx5p-xvqr** on Sep 24, 2020

Package

tensorflow, tensorflow-cpu, tensorflow-gpu (tensorflow)

Affected versions

< 2.3.0

Patched versions

1.15.4, 2.0.3, 2.1.2, 2.2.1, 2.3.1

Description

Impact

The implementation of `SparseFillEmptyRowsGrad` uses a double indexing pattern:

tensorflow/tensorflow/core/kernels/sparse_fill_empty_rows_op.cc
Lines 263 to 269 in `0e68f4d`

```
263     for (int i = 0; i < N; ++i) {
264       // Locate the index of the output of the forward prop associated
265       // with this location in the input of the forward prop.  Copy
266       // the gradient into it.  Mark it as visited.
267       d_values(i) = grad_values(reverse_index_map(i));
268       visited(reverse_index_map(i)) = true;
269     }
```

It is possible for `reverse_index_map(i)` to be an index outside of bounds of `grad_values`, thus resulting in a heap buffer overflow.

Patches

We have patched the issue in `390611e` and will release a patch release for all affected versions.

We recommend users to upgrade to TensorFlow 1.15.4, 2.0.3, 2.1.2, 2.2.1, or 2.3.1.

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 members of the Aivul Team from Qihoo 360.

Severity

High

CVE ID

CVE-2020-15195

Weaknesses

No CWEs