Crash due to invalid shape of grad_values in SparseFillEmptyRowsGrad

Moderate **mihaimaruseac** published **GHSA-9mqp-7v2h-2382** on Sep 24, 2020

Package

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

Affected versions	Patched versions
< 2.3.0	1.15.4, 2.0.3, 2.1.2, 2.2.1, 2.3.1

Description

Impact

The `SparseFillEmptyRowsGrad` implementation has incomplete validation of the shapes of its arguments:

tensorflow/tensorflow/core/kernels/sparse_fill_empty_rows_op.cc
Lines 235 to 241 in `0e68f4d`

```
235     OP_REQUIRES(
236         context, TensorShapeUtils::IsVector(reverse_index_map_t->shape()),
237         errors::InvalidArgument("reverse_index_map must be a vector, saw: ",
238                                 reverse_index_map_t->shape().DebugString()));
239
240     const auto reverse_index_map = reverse_index_map_t->vec<int64>();
241     const auto grad_values = grad_values_t->vec<T>();
```

Although `reverse_index_map_t` and `grad_values_t` are accessed in a similar pattern, only `reverse_index_map_t` is validated to be of proper shape. Hence, malicious users can pass a bad `grad_values_t` to trigger an assertion failure in `vec`, causing denial of service in serving installations.

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 is a variant of GHSA-63xm-rx5p-xvqr

Severity

Moderate

CVE ID

CVE-2020-15194

Weaknesses

No CWEs