Segfault in tf.raw_ops.Switch in eager mode

Moderate **mihaimaruseac** published **GHSA-4g9f-63rx-5cw4** 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 `tf.raw_ops.Switch` operation takes as input a tensor and a boolean and outputs two tensors. Depending on the boolean value, one of the tensors is exactly the input tensor whereas the other one should be an empty tensor.

However, the eager runtime traverses all tensors in the output:

tensorflow/tensorflow/core/common_runtime/eager/kernel_and_device.cc
Lines 308 to 313 in `0e68f4d`

```
308     if (outputs != nullptr) {
309       outputs->clear();
310       for (int i = 0; i < context.num_outputs(); ++i) {
311         outputs->push_back(Tensor(*context.mutable_output(i)));
312       }
313     }
```

Since only one of the tensors is defined, the other one is `nullptr`, hence we are binding a reference to `nullptr`. This is undefined behavior and reported as an error if compiling with `-fsanitize=null`. In this case, this results in a segmentation fault

Patches

We have patched the issue in `da85585` 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

Moderate

CVE ID

CVE-2020-15190

Weaknesses

No CWEs