Segfault by calling session-only ops in eager mode

Moderate **mihaimaruseac** published **GHSA-q8gv-q7wr-9jf8** 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

In eager mode, TensorFlow does not set the session state. Hence, calling `tf.raw_ops.GetSessionHandle` or `tf.raw_ops.GetSessionHandleV2` results in a null pointer dereference:

tensorflow/tensorflow/core/kernels/session_ops.cc
Line 45 in `0e68f4d`

```
45      int64 id = ctx->session_state()->GetNewId();
```

In the above snippet, in eager mode, `ctx->session_state()` returns `nullptr`. Since code immediately dereferences this, we get a segmentation fault.

Patches

We have patched the issue in `9a133d7` and will release patch releases for all versions between 1.15 and 2.3.

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-2020-15204

Weaknesses

No CWEs