Session operations in eager mode lead to null pointer dereferences

Low **mihaimaruseac** published **GHSA-62gx-355r-9fhg** 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

In eager mode (default in TF 2.0 and later), session operations are invalid. However, users could still call the raw ops associated with them and trigger a null pointer dereference:

```
import tensorflow as tf
tf.raw_ops.GetSessionTensor(handle=['\x12\x1a\x07'],dtype=4)
```

```
import tensorflow as tf
tf.raw_ops.DeleteSessionTensor(handle=['\x12\x1a\x07'])
```

The implementation dereferences the session state pointer without checking if it is valid:

```
  OP_REQUIRES_OK(ctx, ctx->session_state()->GetTensor(name, &val));
```

Thus, in eager mode, `ctx->session_state()` is nullptr and the call of the member function is undefined behavior.

Patches

We have patched the issue in GitHub commit ff70c47a396ef1e3cb73c90513da4f5cb71bebba.

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 members of the Aivul Team from Qihoo 360.

Severity

Low

CVE ID

CVE-2021-29518

Weaknesses

No CWEs