Memory leak in dlpack

Low **mihaimaruseac** published **GHSA-8fxw-76px-3rxv** on Sep 24, 2020

Package

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

Affected versions	Patched versions
2.2.0, 2.3.0	2.2.1, 2.3.1

Description

Impact

If a user passes a list of strings to `dlpack.to_dlpack` there is a memory leak following an expected validation failure:

tensorflow/tensorflow/c/eager/dlpack.cc
Lines 100 to 104 in `0e68f4d`

```
100     default:
101       status->status = tensorflow::errors::InvalidArgument(
102           DataType_Name(static_cast<DataType>(data_type)),
103           " is not supported by dlpack");
104       break;
```

The allocated memory is from

tensorflow/tensorflow/c/eager/dlpack.cc
Line 256 in `0e68f4d`

```
256     auto* tf_dlm_tensor_ctx = new TfDlManagedTensorCtx(tensor_ref);
```

The issue occurs because the `status` argument during validation failures is not properly checked:

tensorflow/tensorflow/c/eager/dlpack.cc
Lines 265 to 267 in `0e68f4d`

```
265     dlm_tensor->dl_tensor.data = TFE_TensorHandleDevicePointer(h, status);
266     dlm_tensor->dl_tensor.dtype = GetDlDataType(data_type, status);
267
```

Since each of the above methods can return an error status, the `status` value must be checked before continuing.

Patches

We have patched the issue in `22e07fb` and will release a patch release for all affected versions.

We recommend users to upgrade to TensorFlow 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 discovered during variant analysis of GHSA-rjjg-hgv6-h69v.

Severity

Low

CVE ID

CVE-2020-15192

Weaknesses

No CWEs