Heap out of bounds access in MakeEdge

High **mihaimaruseac** published **GHSA-q263-fvxm-m5mw** on Dec 9, 2020

Package

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

Affected versions	Patched versions
< 2.4.0	1.15.5, 2.0.4, 2.1.3, 2.2.2, 2.3.2, 2.4.0

Description

Impact

Under certain cases, loading a saved model can result in accessing uninitialized memory while building the computation graph. The `MakeEdge` function creates an edge between one output tensor of the `src` node (given by `output_index`) and the input slot of the `dst` node (given by `input_index`). This is only possible if the types of the tensors on both sides coincide, so the function begins by obtaining the corresponding `DataType` values and comparing these for equality:

```
DataType src_out = src->output_type(output_index);
DataType dst_in = dst->input_type(input_index);
//...
```

However, there is no check that the indices point to inside of the arrays they index into. Thus, this can result in accessing data out of bounds of the corresponding heap allocated arrays.

In most scenarios, this can manifest as unitialized data access, but if the index points far away from the boundaries of the arrays this can be used to leak addresses from the library.

Patches

We have patched the issue in GitHub commit 0cc38aaa4064fd9e79101994ce9872c6d91f816b and will release TensorFlow 2.4.0 containing the patch. TensorFlow nightly packages after this commit will also have the issue resolved.

Since this issue also impacts TF versions before 2.4, we will patch all releases between 1.15 and 2.3 inclusive.

For more information

Please consult our security guide for more information regarding the security model and how to contact us with issues and questions.

Severity

High

CVE ID

CVE-2020-26271

Weaknesses

No CWEs