# Uninitialized memory access in Eigen types

Low **mihaimaruseac** published **GHSA-qhxx-j73r-qpm2** 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, a saved model can trigger use of uninitialized values during code execution. This is caused by having tensor buffers be filled with the default value of the type but forgetting to default initialize the quantized floating point types in Eigen:

```
struct QUInt8 {
  QUInt8() {}
  // ...
  uint8_t value;
};

struct QInt16 {
  QInt16() {}
  // ...
  int16_t value;
};

struct QUInt16 {
  QUInt16() {}
  // ...
  uint16_t value;
};

struct QInt32 {
  QInt32() {}
  // ...
  int32_t value;
};
```

## Patches

We have patched the issue in GitHub commit ace0c15a22f7f054abcc1f53eabbcb0a1239a9e2 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**

Low

**CVE ID**

CVE-2020-26266

**Weaknesses**

No CWEs