tensorflow / **tensorflow** Public

Code Issues 2.1k Pull requests 284 Actions Projects 1 ···

Missing validation causes denial of service via `Conv3DBackpropFilterV2`

Low **mihaimaruseac** published **GHSA-hx9q-2mx4-m4pg** on May 17

Package

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

Affected versions	Patched versions
< 2.9.0	2.6.4, 2.7.2, 2.8.1, 2.9.0

Description

Impact

The implementation of `tf.raw_ops.UnsortedSegmentJoin` does not fully validate the input arguments. This results in a `CHECK` -failure which can be used to trigger a denial of service attack:

```
import tensorflow as tf

tf.strings.unsorted_segment_join(
  inputs=['123'],
  segment_ids=[0],
  num_segments=-1)
```

The code assumes `num_segments` is a positive scalar but there is no validation:

```
const Tensor& num_segments_tensor = context->input(2);
auto num_segments = num_segments_tensor.scalar<NUM_SEGMENTS_TYPE>()();
// ...
Tensor* output_tensor = nullptr;
TensorShape output_shape =
    GetOutputShape(input_shape, segment_id_shape, num_segments);
```

Since this value is used to allocate the output tensor, a negative value would result in a `CHECK` -failure (assertion failure), as per TFSA-2021-198.

Patches

We have patched the issue in GitHub commit 84563f265f28b3c36a15335c8b005d405260e943 and GitHub commit 20cb18724b0bf6c09071a3f53434c4eec53cc147.

The fix will be included in TensorFlow 2.9.0. We will also cherrypick this commit on TensorFlow 2.8.1, TensorFlow 2.7.2, and TensorFlow 2.6.4, 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 externally via a GitHub issue.

Severity

Low

CVE ID

CVE-2022-29204

Weaknesses

No CWEs