Integer overflow in `SpaceToBatchND`

High **mihaimaruseac** published **GHSA-jjm6-4vf7-cjh4** 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.SpaceToBatchND` (in all backends such as XLA and handwritten kernels) is vulnerable to an integer overflow:

```
import tensorflow as tf

input = tf.constant(-3.5e+35, shape=[10,19,22], dtype=tf.float32)
block_shape = tf.constant(-1879048192, shape=[2], dtype=tf.int64)
paddings = tf.constant(0, shape=[2,2], dtype=tf.int32)
tf.raw_ops.SpaceToBatchND(input=input, block_shape=block_shape, paddings=paddings)
```

The result of this integer overflow is used to allocate the output tensor, hence we get a denial of service via a `CHECK` -failure (assertion failure), as in TFSA-2021-198.

Patches

We have patched the issue in GitHub commit acd56b8bcb72b163c834ae4f18469047b001fadf.

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 by Neophytos Christou from Secure Systems Lab at Brown University.

Severity

High

CVE ID

CVE-2022-29203

Weaknesses

No CWEs