Segmentation fault when converting a Python string to `tf.float16`

High **mihaimaruseac** published **GHSA-977j-xj7q-2jr9** on Jan 28, 2020

Package

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

Affected versions	Patched versions
>= 1.12.0, < 2.1.0	1.15.2, 2.0.1, 2.1.0

Description

Impact

Converting a string (from Python) to a `tf.float16` value results in a segmentation fault in eager mode as the format checks for this use case are only in the graph mode.

This issue can lead to denial of service in inference/training where a malicious attacker can send a data point which contains a string instead of a `tf.float16` value.

Similar effects can be obtained by manipulating saved models and checkpoints whereby replacing a scalar `tf.float16` value with a scalar string will trigger this issue due to automatic conversions.

This can be easily reproduced by `tf.constant("hello", tf.float16)`, if eager execution is enabled.

Patches

We have patched the vulnerability in GitHub commit 5ac1b9.

We are additionally releasing TensorFlow 1.15.2 and 2.0.1 with this vulnerability patched.

TensorFlow 2.1.0 was released after we fixed the issue, thus it is not affected.

We encourage users to switch to TensorFlow 1.15.2, 2.0.1 or 2.1.0.

For more information

Please consult `SECURITY.md` for more information regarding the security model and how to contact us with issues and questions.

Severity

High

CVE ID

CVE-2020-5215

Weaknesses

No CWEs