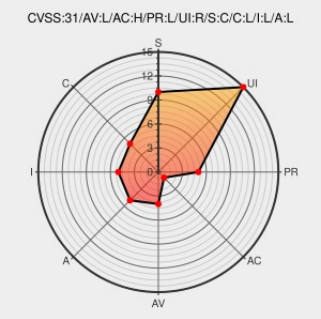
# CVE-2020-5215

Published on: 01/28/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:03 PM UTC

## **CVE-2020-5215** - advisory for GHSA-977j-xj7q-2jr9

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Tensorflow from Google contain the following vulnerability:

In TensorFlow before 1.15.2 and 2.0.1, 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. This issue is patched in TensorFlow 1.15.1 and 2.0.1 with this vulnerability patched. TensorFlow 2.1.0 was released after we fixed the issue, thus it is not affected. Users are encouraged to switch to TensorFlow 1.15.1, 2.0.1 or 2.1.0.

CVE-2020-5215 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **TensorFlow** - **TensorFlow** version **< 1.15.2**

Affected Vendor/Software: **TensorFlow** - **TensorFlow** version **= 2.0.0**

### CVSS3 Score: 7.5 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| NETWORK | LOW | NONE | NONE |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | NONE | NONE | HIGH |

### CVSS2 Score: 4.3 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|

| NETWORK | MEDIUM | NONE |
|---|---|---|
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| NONE | NONE | PARTIAL |

## CVE References

| Description | Tags | Link |
|---|---|---|
| Release TensorFlow 1.15.2 · tensorflow/tensorflow · GitHub | Release Notes, github.com, text/html | MISC github.com/tensorflow/tensorflow/releases/tag/v1.15.2 |
| Segmentation fault when converting a Python string to `tf.float16` · Advisory · tensorflow/tensorflow · GitHub | Exploit, Patch, Third Party Advisory, github.com, text/html | CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-977j-xj7q-2 |
| Release TensorFlow 2.0.1 · tensorflow/tensorflow · GitHub | Release Notes, github.com, text/html | MISC github.com/tensorflow/tensorflow/releases/tag/v2.0.1 |
| Fix segfault when attempting to convert string to float16. · tensorflow/tensorflow@5ac1b9e · GitHub | Patch, github.com, text/html | MISC github.com/tensorflow/tensorflow/commit/5ac1b9e24ff6afc465756edf845d2e9660bd3 |



## Related QID Numbers

983114 Python (pip) Security Update for tensorflow-gpu (GHSA-977j-xj7q-2jr9)

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Google | Tensorflow | All | All | All | All |
| Application | Google | Tensorflow | All | All | All | All |

cpe:2.3:a:google:tensorflow:*:*:*:*:*:*:*:*:

cpe:2.3:a:google:tensorflow:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

**CVE.report and Source URL Uptime Status status.cve.report**