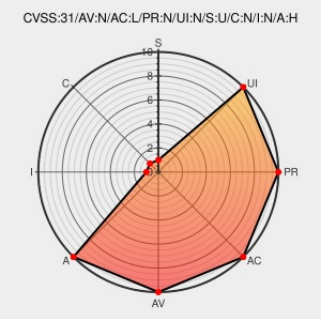
# CVE-2020-15203

Published on: 09/25/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 05:26:00 PM UTC

## **CVE-2020-15203** - advisory for GHSA-xmq7-7fxm-rr79

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




Certain versions of Tensorflow from Google contain the following vulnerability:

In Tensorflow before versions 1.15.4, 2.0.3, 2.1.2, 2.2.1 and 2.3.1, by controlling the `fill` argument of tf.strings.as_string, a malicious attacker is able to trigger a format string vulnerability due to the way the internal format use in a `printf` call is constructed. This may result in segmentation fault. The issue is patched in commit 33be22c65d86256e6826666662e40dbdfe70ee83, and is released in TensorFlow versions 1.15.4, 2.0.3, 2.1.2, 2.2.1, or 2.3.1.

CVE-2020-15203 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **tensorflow** - **tensorflow** version **< 1.15.4**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.0.0, < 2.0.3**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.1.0, < 2.1.2**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.2.0, < 2.2.1**

Affected Vendor/Software: **tensorflow** - **tensorflow** version **>= 2.3.0, < 2.3.1**

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: 5 - MEDIUM

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

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

## CVE References

| Description | Tags | Link |
|---|---|---|
| Format-string vulnerability in TensorFlow's `as_string` · Advisory · tensorflow/tensorflow · GitHub | Exploit, Third Party Advisory, github.com, text/html | CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-xmq7-7fxm |
| Prevent format string vulnerability in `tf.strings.as_string`. · tensorflow/tensorflow@33be22c · GitHub | Patch, Third Party Advisory, github.com, text/html | MISC github.com/tensorflow/tensorflow/commit/33be22c65d86256e6826666662e40dbdfe7 |
| Release TensorFlow 2.3.1 · tensorflow/tensorflow · GitHub | Third Party Advisory, github.com, text/html | MISC github.com/tensorflow/tensorflow/releases/tag/v2.3.1 |
| [security-announce] openSUSE-SU-2020:1766-1: moderate: Security update f | lists.opensuse.org, text/html | SUSE openSUSE-SU-2020:1766 |



## Related QID Numbers

980054 Python (pip) Security Update for tensorflow-gpu (GHSA-xmq7-7fxm-rr79)

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Google | Tensorflow | All | All | All | All |
| Operating System | Opensuse | Leap | 15.2 | All | All | All |
| Application | Tensorflow | Tensorflow | All | All | All | All |
| Application | Tensorflow | Tensorflow | All | All | All | All |

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

cpe:2.3:o:opensuse:leap:15.2:*:*:*:*:*:*:*:

cpe:2.3:a:tensorflow:tensorflow:*:*:*:*:-:*:*:*:

cpe:2.3:a:tensorflow:tensorflow:*:*:*:*:-:*:*:*:

No vendor comments have been submitted for this CVE

## Social Mentions

| Source | Title | Posted (UTC) |
| --- | --- | --- |
| @LinInfoSec | Tensorflow - CVE-2020-15203: github.com/tensorflow/ten… | 2021-09-16 19:45:17 |

← Previous ID

Next ID→