

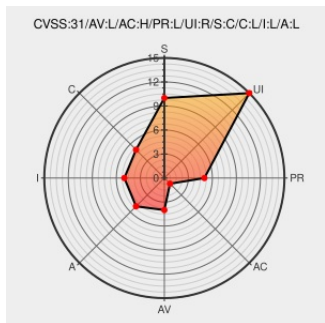


CVE-2020-5215

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
---------------	-------------------	----------------

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-
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/5ac1b9e24ff6afc465756edf845d2e9660bd

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

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→

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)