



CVE-2020-15207

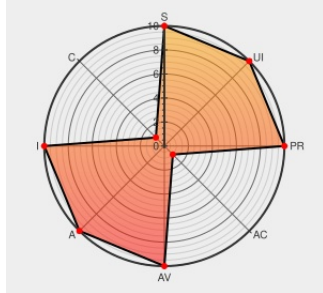
Published on: 09/25/2020 12:00:00 AM UTC

Last Modified on: 11/18/2021 05:27:00 PM UTC

CVE-2020-15207 - advisory for GHSA-q4qf-3fc6-8x34

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:31/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:H



Certain versions of [Tensorflow](#) from [Google](#) contain the following vulnerability:

In tensorflow-lite before versions 1.15.4, 2.0.3, 2.1.2, 2.2.1 and 2.3.1, to mimic Python's indexing with negative values, TFLite uses `ResolveAxis` to convert negative values to positive indices. However, the only check that the converted index is now valid is only present in debug builds. If the `DCHECK` does not trigger, then code execution

moves ahead with a negative index. This, in turn, results in accessing data out of bounds which results in segfaults and/or data corruption. The issue is patched in commit 2d88f470dea2671b430884260f3626b1fe99830a, and is released in TensorFlow versions 1.15.4, 2.0.3, 2.1.2, 2.2.1, or 2.3.1.

CVE-2020-15207 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** 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: **9 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6.8 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
[tflite] Ensure `ResolveAxis` properly handles negative inputs. · tensorflow/tensorflow@2d88f47 · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/tensorflow/tensorflow/commit/2d88f470dea2671b430884260f3626b1fe998
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
Segfault and data corruption caused by negative indexing in TFLite · Advisory · tensorflow/tensorflow · GitHub	Exploit Third Party Advisory github.com text/html	 CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-q4qf-3fc6-8

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

980057 Python (pip) Security Update for tensorflow-gpu (GHSA-q4qf-3fc6-8x34)

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:*:*:*:lite:*:*:
```

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

cpe:2.3:a:tensorflow:tensorflow:*:*:*:lite:*:*:

cpe:2.3:a:tensorflow:tensorflow:*:*:*:*:lite:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @LinInfoSec	Tensorflow - CVE-2020-15207: github.com/tensorflow/ten...	2021-08-17 14:46:21

[← Previous ID](#)

[Next ID→](#)

© CVE.report 2023   |

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](#)