

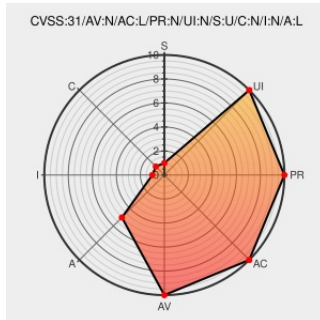


CVE-2020-15194

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

Last Modified on: 08/17/2021 01:21:00 PM UTC

CVE-2020-15194 - advisory for GHSA-9mqp-7v2h-2382

[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, the ``SparseFillEmptyRowsGrad`` implementation has incomplete validation of the shapes of its arguments. Although ``reverse_index_map_t`` and ``grad_values_t`` are accessed in a similar pattern, only ``reverse_index_map_t`` is validated to be of proper shape. Hence,

malicious users can pass a bad ``grad_values_t`` to trigger an assertion failure in ``vec``, causing denial of service in serving installations. The issue is patched in commit 390611e0d45c5793c7066110af37c8514e6a6c54, and is released in TensorFlow versions 1.15.4, 2.0.3, 2.1.2, 2.2.1, or 2.3.1."

CVE-2020-15194 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** 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: **5.3 - MEDIUM**

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

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
Fix heap buffer overflow in `tf.raw_ops.SparseFillEmptyRowsGrad`. · tensorflow/tensorflow@390611e · GitHub	Patch Third Party Advisory github.com text/html	 MISC github.com/tensorflow/tensorflow/commit/390611e0d45c5793c7066110af37c
Release TensorFlow 2.3.1 · tensorflow/tensorflow · GitHub	Release Notes Third Party Advisory github.com text/html	 MISC github.com/tensorflow/tensorflow/releases/tag/v2.3.1
Crash due to invalid shape of grad_values in SparseFillEmptyRowsGrad · Advisory · tensorflow/tensorflow · GitHub	Exploit Patch Third Party Advisory github.com text/html	 CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-9mqp-7v2h-2382
[security-announce] openSUSE-SU-2020:1766-1: moderate: Security update f	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2020:1766

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

981474 Python (pip) Security Update for tensorflow-gpu (GHSA-9mqp-7v2h-2382)

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
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:o:opensuse:leap:15.2.*:*:*:*:*:
cpe:2.3:a:tensorflow:tensorflow:*:*:*:*:*:
cpe:2.3:a:tensorflow:tensorflow:*:*:*:*:*:

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

cpe:2.3:o:opensuse:leap:15.2.*:*:*:*:*:
cpe:2.3:o:opensuse:leap:15.2.*:*:*:*:*:
cpe:2.3:a:tensorflow:tensorflow:*:*:*:_:*:*:
cpe:2.3:a:tensorflow:tensorflow:*:*:*:_:*:*:

cpe:2.3:o:opensuse:leap:15.2.*:*:*:*:*:
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)
--------	-------	--------------

Source	Title	Posted (UTC)
--------	-------	--------------

Source	Title	Posted (UTC)
--------	-------	--------------

[← 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