

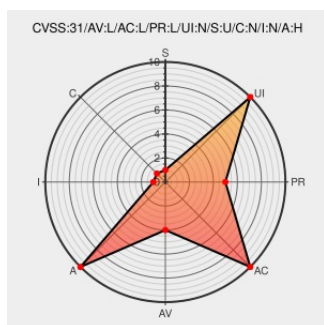


CVE-2022-29206

Published on: Not Yet Published

Last Modified on: 06/02/2022 07:37:00 PM UTC

CVE-2022-29206 - advisory for GHSA-rc9w-5c64-9vqq

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

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

TensorFlow is an open source platform for machine learning. Prior to versions 2.9.0, 2.8.1, 2.7.2, and 2.6.4, the implementation of ``tf.raw_ops.SparseTensorDenseAdd`` does not fully validate the input arguments. In this case, a reference gets bound to a ``nullptr`` during kernel execution. This is undefined behavior. Versions 2.9.0, 2.8.1, 2.7.2, and 2.6.4 contain a patch for this issue.

CVE-2022-29206 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version < 2.6.4

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version >= 2.7.0rc0, < 2.7.2

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version >= 2.8.0rc0, < 2.8.1

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version >= 2.9.0rc0, < 2.9.0

CVSS3 Score: **5.5 - MEDIUM**

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

CVSS2 Score: **2.1 - LOW**

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality	Integrity	Availability

[illegible]

cpe:2.3:a:google:tensorflow:2.7.0:rc1:~::~::~:
cpe:2.3:a:google:tensorflow:2.8.0:-::~::~:
cpe:2.3:a:google:tensorflow:2.8.0:rc0:~::~::~:
cpe:2.3:a:google:tensorflow:2.8.0:rc1:~::~::~:
cpe:2.3:a:google:tensorflow:2.9.0:rc0:~::~::~:
cpe:2.3:a:google:tensorflow:2.9.0:rc1:~::~::~:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-29206 : TensorFlow is an open source platform for machine learning. Prior to versions 2.9.0, 2.8.1, 2.7.2,... twitter.com/i/web/status/1...	2022-05-20 22:21:27
 @LinInfoSec	Tensorflow - CVE-2022-29206: github.com/tensorflow/ten...	2022-05-21 01:01:28
 @threatmeter	CVE-2022-29206 TensorFlow is an open source platform for machine learning. Prior to versions 2.9.0, 2.8.1, 2.7.2, a... twitter.com/i/web/status/1...	2022-05-21 07:10:00
 /r/netcve	CVE-2022-29206	2022-05-20 23:38:40

[← 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](#)