

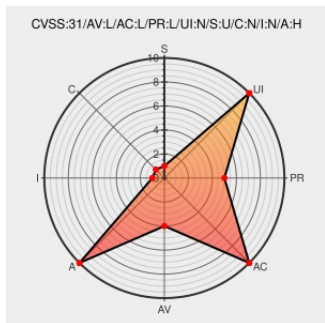


CVE-2022-29203

Published on: Not Yet Published

Last Modified on: 06/02/2022 07:16:00 PM UTC

CVE-2022-29203 - advisory for GHSA-jjm6-4vf7-cjh4

[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.SpaceToBatchND`` (in all backends such as XLA and handwritten kernels) is vulnerable to an integer overflow: The result of this integer overflow is used to allocate the output tensor, hence we get a denial of service via a ``CHECK``-failure (assertion failure), as in TFSA-2021-198. Versions 2.9.0, 2.8.1, 2.7.2, and 2.6.4 contain a patch for this issue.

CVE-2022-29203 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

cpe:2.3:a:google:tensorflow:2.7.0:rc0:~::~~::~~::~~::~::
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-2022-29203 : 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 22:51:49
 @LinInfoSec	Tensorflow - CVE-2022-29203: github.com/tensorflow/ten...	2022-05-21 01:01:28
 /r/netcve	CVE-2022-29203	2022-05-20 23:38:44