

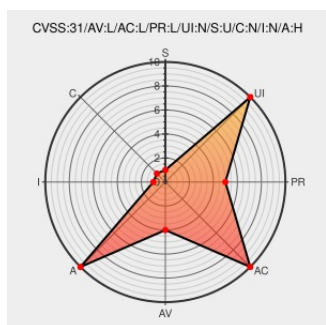


CVE-2022-29200

Published on: Not Yet Published

Last Modified on: 07/21/2023 04:41:00 PM UTC

CVE-2022-29200 - advisory for GHSA-2vv3-56qg-g2cf

[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.LSTMBlockCell`` does not fully validate the input arguments. This results in a ``CHECK``-failure which can be used to trigger a denial of service attack. The code does not validate the ranks

of any of the arguments to this API call. This results in ``CHECK``-failures when the elements of the tensor are accessed. Versions 2.9.0, 2.8.1, 2.7.2, and 2.6.4 contain a patch for this issue.

CVE-2022-29200 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 Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Release TensorFlow 2.8.1 · tensorflow/tensorflow · GitHub	github.com text/html	 MISC github.com/tensorflow/tensorflow/releases/tag/v2.8.1
Release TensorFlow 2.9.0 · tensorflow/tensorflow · GitHub	github.com text/html	 MISC github.com/tensorflow/tensorflow/releases/tag/v2.9.0
Release TensorFlow 2.7.2 · tensorflow/tensorflow · GitHub	github.com text/html	 MISC github.com/tensorflow/tensorflow/releases/tag/v2.7.2
tensorflow/lstm_ops.cc at f3b9bf4c3c0597563b289c0512e98d4ce81f886e · tensorflow/tensorflow · GitHub	github.com text/html	 MISC github.com/tensorflow/tensorflow/blob/f3b9bf4c3c0597563b289c0512e98d4ce81f886e/tensorflow/tensorflow
Release TensorFlow 2.6.4 · tensorflow/tensorflow · GitHub	github.com text/html	 MISC github.com/tensorflow/tensorflow/releases/tag/v2.6.4
Fix security vulnerability with LSTMBlockCellOp · tensorflow/tensorflow@8034040 · GitHub	github.com text/html	 MISC github.com/tensorflow/tensorflow/commit/803404044ae7a1efac48b2
Missing validation causes denial of service via `LSTMBlockCell` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	 CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-2v9p-433p-933p

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.7.0	rc0	All	All
Application	Google	Tensorflow	2.7.0	rc1	All	All
Application	Google	Tensorflow	2.8.0	-	All	All
Application	Google	Tensorflow	2.8.0	rc0	All	All
Application	Google	Tensorflow	2.8.0	rc1	All	All
Application	Google	Tensorflow	2.9.0	rc0	All	All
Application	Google	Tensorflow	2.9.0	rc1	All	All

```
cpe:2.3:a:google:tensorflow:*:*:*:*:*:*:*:
```

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-2022-29200 : 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 21:36:51
 @LinInfoSec	Tensorflow - CVE-2022-29200: github.com/tensorflow/ten...	2022-05-21 01:01:30
 /r/netcve	CVE-2022-29200	2022-05-20 22:38:55