

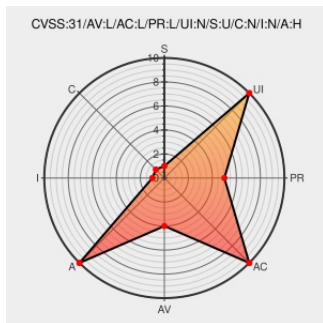


CVE-2021-37686

Published on: 08/12/2021 12:00:00 AM UTC

Last Modified on: 08/18/2021 08:42:00 PM UTC

CVE-2021-37686 - advisory for GHSA-mhhc-q96p-mfm9

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

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

TensorFlow is an end-to-end open source platform for machine learning. In affected versions the strided slice implementation in TFLite has a logic bug which can allow an attacker to trigger an infinite loop. This arises from newly introduced support for [ellipsis in axis definition]

(<https://github.com/tensorflow/tensorflow/blob/149562d49faa709ea80df1d99fc41d005b81082a/L122>). An attacker can craft a model such that `ellipsis\_end\_idx` is smaller than `i` (e.g., always negative). In this case, the inner loop does not increase `i` and the `continue` statement causes execution to skip over the preincrement at the end of the outer loop. We have patched the issue in GitHub commit [dfa22b348b70bb89d6d6ec0ff53973bacb4f4695](#). TensorFlow 2.6.0 is the only affected version.

CVE-2021-37686 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [tensorflow](#) - tensorflow version = 2.6.0

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

Confidentiality Impact

NONE

Integrity Impact

NONE

Availability Impact

PARTIAL

CVE References

Description

Prevent a division by 0 in average ops. · tensorflow/tensorflow@dfa22b3 · GitHub

Tags

github.com

text/html

Link

MISC

github.com/tensorflow/tensorflow/commit/dfa22b348b70bb89d6d6ec0ff53973bac4f4695

Description

Infinite loop in TFLite · Advisory · tensorflow/tensorflow · GitHub

Tags

github.com

text/html

Link

CONFIRM

github.com/tensorflow/tensorflow/security/advisories/GHSA-mhhc-q96p-mfm9

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

981550 Python (pip) Security Update for tensorflow-gpu (GHSA-mhhc-q96p-mfm9)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	2.5.0	All	All	All
Application	Google	Tensorflow	2.6.0	rc0	All	All
Application	Google	Tensorflow	2.6.0	rc1	All	All
Application	Google	Tensorflow	2.6.0	rc2	All	All

cpe:2.3:a:google:tensorflow:*.***.***.***:

cpe:2.3:a:google:tensorflow:2.5.0:*.***.***.***:

cpe:2.3:a:google:tensorflow:2.6.0:rc0:*.***.***.***:

cpe:2.3:a:google:tensorflow:2.6.0:rc1:*.***.***.***:

cpe:2.3:a:google:tensorflow:2.6.0:rc2:*.***.***.***:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@LinInfoSec	Tensorflow - CVE-2021-37686: github.com/tensorflow/ten...	2021-08-13 00:52:17

© [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](#)