

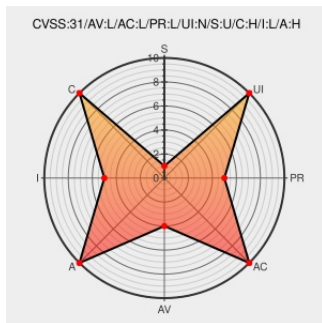


CVE-2021-37654

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

Last Modified on: 08/18/2021 02:30:00 PM UTC

CVE-2021-37654 - advisory for GHSA-2r8p-fg3c-wcj4

[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 an attacker can trigger a crash via a `CHECK`-fail in debug builds of TensorFlow using `tf.raw\_ops.ResourceGather` or a read from outside the bounds of heap allocated data in the same API in a release build. The

[implementation]

(<https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1ddeb/L668>) does not check that the `batch\_dims` value that the user supplies is less than the rank of the input tensor. Since the implementation uses several for loops over the dimensions of `tensor`, this results in reading data from outside the bounds of heap allocated buffer backing the tensor. We have patched the issue in GitHub commit [bc9c546ce7015c57c2f15c168b3d9201de679a1d](#). The fix will be included in TensorFlow 2.6.0. We will also cherrypick this commit on TensorFlow 2.5.1, TensorFlow 2.4.3, and TensorFlow 2.3.4, as these are also affected and still in supported range.

CVE-2021-37654 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: tensorflow - tensorflow version $\geq 2.5.0$, $< 2.5.1$

Affected Vendor/Software: tensorflow - tensorflow version $\geq 2.4.0$, $< 2.4.3$

Affected Vendor/Software: tensorflow - tensorflow version $< 2.3.4$

CVSS3 Score: **7.1 - HIGH**

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

No further comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-37654 : TensorFlow is an end-to-end open source platform for machine learning. In affected versions an att... twitter.com/i/web/status/1...	2021-08-12 20:36:47
 @LinInfoSec	Tensorflow - CVE-2021-37654: github.com/tensorflow/ten...	2021-08-12 22:40:41

[← 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](#)