



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

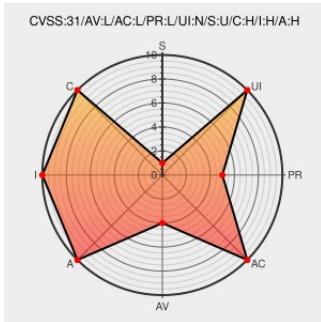
Last Modified on: 10/25/2022 04:03:00 PM UTC

CVE-2021-37652 - advisory for GHSA-m7fm-4jfh-jrg6

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 implementation for ``tf.raw_ops.BoostedTreesCreateEnsemble`` can result in a use after free error if an attacker supplies specially crafted arguments. The [implementation]

(<https://github.com/tensorflow/tensorflow/blob/f24faa153ad31a4b51578f8181d3aaab77a1dde>). It uses a reference counted resource and decrements the refcount if the initialization fails, as it should. However, when the code was written, the resource was represented as a naked pointer but later refactoring has changed it to be a smart pointer. Thus, when the pointer leaves the scope, a subsequent `free`-ing of the resource occurs, but this fails to take into account that the refcount has already reached 0, thus the resource has been already freed. During this double-free process, members of the resource object are accessed for cleanup but they are invalid as the entire resource has been freed. We have patched the issue in GitHub commit [5ecec9c6fbdbc6be03295685190a45e7eee726ab](https://github.com/tensorflow/tensorflow/commit/5ecec9c6fbdbc6be03295685190a45e7eee726ab). 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-2021-37652 has been assigned by  security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: tensorflow - tensorflow version >= 2.5.0, < 2.5.1

Affected Vendor/Software: tensorflow - tensorflow version >= 2.4.0, < 2.4.3

Affected Vendor/Software: tensorflow - tensorflow version < 2.3.4

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH
CVSS2 Score: 4.6 - MEDIUM			
Access Vector	Access Complexity	Authentication	
LOCAL	LOW	NONE	
Confidentiality Impact	Integrity Impact	Availability Impact	
PARTIAL	PARTIAL	PARTIAL	

CVE References

Description	Tags	Link
Prevent use after free. · tensorflow/tensorflow@5ecec9c · GitHub	github.com text/html	 MISC github.com/tensorflow/tensorflow/commit/5ecec9c6fbdbc6be03295685190a45e7eee726ab
Use after free in boosted trees creation · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	 CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-m7fm-4jfh-jrg6

Prevent use after free. ·
tensorflow/tensorflow@5ecec9c
· GitHub

Use after free in boosted trees
creation · Advisory ·
tensorflow/tensorflow · GitHub

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

981521 Python (pip) Security Update for tensorflow-gpu (GHSA-m7fm-4jfh-jrg6)

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:*. *.*.*.*.*.*.*.*:						

```
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)
 @CVereport	CVE-2021-37652 : TensorFlow is an end-to-end open source platform for machine learning. In affected versions the im... twitter.com/i/web/status/1...	2021-08-12 21:21:32

[← 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](#)