

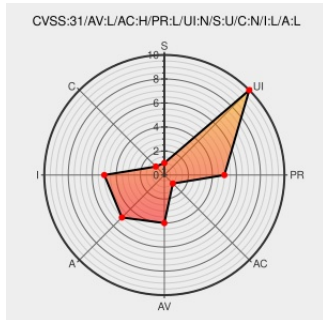


CVE-2021-29612

Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 10/25/2022 08:07:00 PM UTC

CVE-2021-29612 - advisory for GHSA-2xgj-xhgf-ggjjv

[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. An attacker can trigger a heap buffer overflow in Eigen implementation of ``tf.raw_ops.BandedTriangularSolve``. The

implementation(<https://github.com/tensorflow/tensorflow/blob/eccb7ec454e6617738554a255d7L278>) calls ``ValidateInputTensors`` for input validation but fails to validate that the two tensors are not empty. Furthermore, since ``OP_REQUIRES`` macro only stops execution of current function after setting ``ctx->status()`` to a non-OK value, callers of helper functions that use ``OP_REQUIRES`` must check value of ``ctx->status()`` before continuing. This doesn't happen in this op's implementation(<https://github.com/tensorflow/tensorflow/blob/eccb7ec454e6617738554a255d7>) hence the validation that is present is also not effective. The fix will be included in TensorFlow 2.5.0. We will also cherry-pick this commit on TensorFlow 2.4.2, TensorFlow 2.3.3, TensorFlow 2.2.3 and TensorFlow 2.1.4, as these are also affected and still in supported range.

CVE-2021-29612 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: tensorflow - tensorflow version < 2.1.4

Affected Vendor/Software: tensorflow - tensorflow version >= 2.2.0, < 2.2.3

Affected Vendor/Software: tensorflow - tensorflow version >= 2.3.0, < 2.3.3

Affected Vendor/Software: tensorflow - tensorflow version >= 2.4.0, < 2.4.2

CVSS3 Score: **7.8 - HIGH**

Attack
Vector

LOCAL

Attack
Complexity

LOW

Privileges
Required

LOW

User
Interaction

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
Heap buffer overflow in `BandedTriangularSolve` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-2xgj-xhgf-ggfv
Fix OOB issue with `tf.raw_ops.SparseSparseMinimum` · tensorflow/tensorflow@ba6822b · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/ba6822bd7b7324ba201a28b2f278c29a98edbe
Ensure validation sticks in banded_triangular_solve_op · tensorflow/tensorflow@0ab2907 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/0ab290774f91a23bebe30a358fde4e53ab4876
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
982443 Python (pip) Security Update for tensorflow-gpu (GHSA-2xgj-xhgf-ggfv)

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Tensorflow	All	All	All	All
cpe:2.3:a:google:tensorflow:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← 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](#)