



CVE-2022-23589

Published on: 02/04/2022 12:00:00 AM UTC

Last Modified on: 02/10/2022 06:00:00 PM UTC

CVE-2022-23589 - advisory for GHSA-9px9-73fg-3fqp

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

CVSS:31/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H



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

Tensorflow is an Open Source Machine Learning Framework. Under certain scenarios, Grappler component of TensorFlow can trigger a null pointer dereference. There are 2 places where this can occur, for the same malicious alteration of a `SavedModel` file (fixing the first one would trigger the same dereference in the second place). First, during

constant folding, the `GraphDef` might not have the required nodes for the binary operation. If a node is missing, the corresponding `mul\_\*child` would be null, and the dereference in the subsequent line would be incorrect. We have a similar issue during `IsIdentityConsumingSwitch`. The fix will be included in TensorFlow 2.8.0. We will also cherry-pick this commit on TensorFlow 2.7.1, TensorFlow 2.6.3, and TensorFlow 2.5.3, as these are also affected and still in supported range.

CVE-2022-23589 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [tensorflow](#) - tensorflow version $\geq 2.7.0$, $< 2.7.1$

Affected Vendor/Software: [tensorflow](#) - tensorflow version $\geq 2.6.0$, $< 2.6.3$

Affected Vendor/Software: [tensorflow](#) - tensorflow version $< 2.5.3$

CVSS3 Score: **6.5 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: **4 - MEDIUM**

Access

Access

Authentication

Vector	Complexity	
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
tensorflow/mutable_graph_view.cc at a1320ec1eac186da1d03f033109191f715b2b130 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/a1320ec1eac186da1d03f033109191f715b2b130/tensorflow/tensorflow/mutable_graph_view.cc
Prevent null pointer dereference in constant folding. · tensorflow/tensorflow@0a365c0 · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/0a365c029e437be0349c0a365c029e437be0349c
Null pointer dereference in Grappler's `IsConstant` · Advisory · tensorflow/tensorflow · GitHub	github.com text/html	CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-9p3p-3p3p-3p3p
tensorflow/constant_folding.cc at a1320ec1eac186da1d03f033109191f715b2b130 · tensorflow/tensorflow · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/blob/a1320ec1eac186da1d03f033109191f715b2b130/tensorflow/tensorflow/constant_folding.cc
Prevent null pointer dereference in `mutable_graph_view` · tensorflow/tensorflow@045deec · GitHub	github.com text/html	MISC github.com/tensorflow/tensorflow/commit/045deec1cbdebb27d817045deec1cbdebb27d8170

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	2.7.0	All	All	All
Application	Google	Tensorflow	All	All	All	All
Application	Google	Tensorflow	All	All	All	All
cpe:2.3:a:google:tensorflow:2.7.0:*:*:*:*:*						
cpe:2.3:a:google:tensorflow:*:*:*:*:*						
cpe:2.3:a:google:tensorflow:*:*:*:*:*						

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-23589 : Tensorflow is an Open Source Machine Learning Framework. Under certain scenarios, Grappler compone... twitter.com/i/web/status/1...	2022-02-04 22:51:34
 @LinInfoSec	Tensorflow - CVE-2022-23589: github.com/tensorflow/ten...	2022-02-05 02:00:12
 /r/netcve	CVE-2022-23589	2022-02-04 23:38:46
← 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](#)