



# CVE-2022-35991

Published on: Not Yet Published

Last Modified on: 09/20/2022 02:50:00 PM UTC

## CVE-2022-35991 - advisory for GHSA-vm7x-4qhj-rrcq

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

CVSS:31/AV:N/AC:H/PR:N/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 platform for machine learning. When `TensorListScatter` and `TensorListScatterV2` receive an `element\_shape` of a rank greater than one, they give a `CHECK` fail that can trigger a denial of service attack. We have patched the issue in GitHub commit [bb03fdf4aae944ab2e4b35c7daa051068a8b7f61](#). The fix will be included in TensorFlow 2.10.0. We will also cherry-pick this commit on TensorFlow 2.9.1, TensorFlow 2.8.1, and TensorFlow 2.7.2, as these are also affected and still in supported range. There are no known workarounds for this issue.

CVE-2022-35991 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version < 2.7.2

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version >= 2.8.0, < 2.8.1

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version >= 2.9.0, < 2.9.1

CVSS3 Score: **7.5 - HIGH**

| Attack Vector    | Attack Complexity      | Privileges Required | User Interaction    |
|------------------|------------------------|---------------------|---------------------|
| <b>NETWORK</b>   | <b>LOW</b>             | <b>NONE</b>         | <b>NONE</b>         |
| Scope            | Confidentiality Impact | Integrity Impact    | Availability Impact |
| <b>UNCHANGED</b> | <b>NONE</b>            | <b>NONE</b>         | <b>HIGH</b>         |

## CVE References

| Description                                                                | Tags                                                    | Link                                                                                             |
|----------------------------------------------------------------------------|---------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| `CHECK` fail in `TensorListScatter` and `TensorListScatterV2` · Advisory · | <a href="#">github.com</a><br><a href="#">text/html</a> | <a href="#">CONFIRM github.com/tensorflow/tensorflow/security/advisories/GHSA-vm7x-4qhj-rrcq</a> |

Check for element\_shape in  
TensorListScatter and  
TensorListScatterV2 ·  
tensorflow/tensorflow@bb03fdf ·  
GitHub

[github.com](#)  
[text/html](#)

 **MISC**  
[github.com/tensorflow/tensorflow/commit/bb03fdf4aae944ab2e4b35c7daa051068a8b7f61](https://github.com/tensorflow/tensorflow/commit/bb03fdf4aae944ab2e4b35c7daa051068a8b7f61)

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](mailto:comment@cve.report).

## Related QID Numbers

**691141** Free Berkeley Software Distribution (FreeBSD) Security Update for py (ae132c6c-d716-11ed-956f-7054d21a9e2a)

## Known Affected Configurations (CPE V2.3)

| Type                                           | Vendor                 | Product                    | Version | Update | Edition | Language |
|------------------------------------------------|------------------------|----------------------------|---------|--------|---------|----------|
| Application                                    | <a href="#">Google</a> | <a href="#">Tensorflow</a> | All     | All    | All     | All      |
| Application                                    | <a href="#">Google</a> | <a href="#">Tensorflow</a> | 2.10    | rc0    | All     | All      |
| Application                                    | <a href="#">Google</a> | <a href="#">Tensorflow</a> | 2.10    | rc1    | All     | All      |
| Application                                    | <a href="#">Google</a> | <a href="#">Tensorflow</a> | 2.10    | rc2    | All     | All      |
| Application                                    | <a href="#">Google</a> | <a href="#">Tensorflow</a> | 2.10    | rc3    | All     | All      |
| cpe:2.3:a:google:tensorflow:*.:*:*:*:*:        |                        |                            |         |        |         |          |
| cpe:2.3:a:google:tensorflow:2.10:rc0:*.:*:*:*: |                        |                            |         |        |         |          |
| cpe:2.3:a:google:tensorflow:2.10:rc1:*.:*:*:*: |                        |                            |         |        |         |          |
| cpe:2.3:a:google:tensorflow:2.10:rc2:*.:*:*:*: |                        |                            |         |        |         |          |
| cpe:2.3:a:google:tensorflow:2.10:rc3:*.:*:*:*: |                        |                            |         |        |         |          |

No vendor comments have been submitted for this CVE

## Social Mentions

| Source                                                                                        | Title                                                                                                                                                                                                    | Posted (UTC)           |
|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
|  @CVEreport | CVE-2022-35991 : TensorFlow is an open source platform for machine learning. When `TensorListScatter` and `TensorLi... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-09-16<br>22:25:53 |
|  /r/netcve  | <a href="#">CVE-2022-35991</a>                                                                                                                                                                           | 2022-09-16<br>23:38:59 |

[← Previous ID](#)

[Next ID →](#)

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](#)