

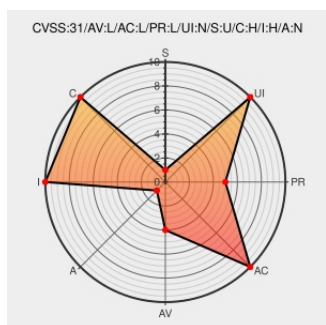


# CVE-2022-23563

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

Last Modified on: 07/13/2023 02:28:00 PM UTC

## CVE-2022-23563 - advisory for GHSA-wc4g-r73w-x8mm

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

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

Tensorflow is an Open Source Machine Learning Framework. In multiple places, TensorFlow uses ``tempfile.mktemp`` to create temporary files. While this is acceptable in testing, in utilities and libraries it is dangerous as a different process can create the file between the check for the filename in ``mktemp`` and the actual creation of the file by a subsequent operation (a TOC/TOU type of weakness). In several instances, TensorFlow was supposed to actually create a temporary directory instead of a file. This logic bug is hidden away by the ``mktemp`` function usage. We have patched the issue in several commits, replacing ``mktemp`` with the safer ``mkstemp``/``mkdtemp`` functions, according to the usage pattern. Users are advised to upgrade as soon as possible.

CVE-2022-23563 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version `>= 2.7.0, < 2.7.1`

Affected Vendor/Software: [tensorflow](#) - **tensorflow** version `>= 2.6.0, < 2.6.3`

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

CVSS3 Score: **6.3 - MEDIUM**

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

CVSS2 Score: **3.3 - LOW**

| Access Vector | Access Complexity | Authentication |
|---------------|-------------------|----------------|
|---------------|-------------------|----------------|

|                        |                  |                     |
|------------------------|------------------|---------------------|
| LOCAL                  | MEDIUM           | NONE                |
| Confidentiality Impact | Integrity Impact | Availability Impact |
| PARTIAL                | PARTIAL          | NONE                |

### CVE References

| Description                                                         | Tags                                                    | Link                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Insecure temporary file · Advisory · tensorflow/tensorflow · GitHub | <a href="#">github.com</a><br><a href="#">text/html</a> |  CONFIRM<br><a href="https://github.com/tensorflow/tensorflow/security/advisories/GHSA-wc4g-r73w-x8mm">github.com/tensorflow/tensorflow/security/advisories/GHSA-wc4g-r73w-x8mm</a> |

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).

There are currently no QIDs associated with this CVE

### Known Affected Configurations (CPE V2.3)

| Type                                     | Vendor                 | Product                    | Version | Update | Edition | Language |
|------------------------------------------|------------------------|----------------------------|---------|--------|---------|----------|
| Application                              | <a href="#">Google</a> | <a href="#">Tensorflow</a> | 2.7.0   | All    | All     | All      |
| Application                              | <a href="#">Google</a> | <a href="#">Tensorflow</a> | All     | All    | All     | All      |
| Application                              | <a href="#">Google</a> | <a href="#">Tensorflow</a> | 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-2022-23563 : Tensorflow is an Open Source Machine Learning Framework. In multiple places, TensorFlow uses `temp... <a href="https://twitter.com/i/web/status/1...">twitter.com/i/web/status/1...</a> | 2022-02-04 22:43:48 |
|  @LinInfoSec | Tensorflow - CVE-2022-23563: <a href="https://github.com/tensorflow/ten...">github.com/tensorflow/ten...</a>                                                                                             | 2022-02-05 02:00:15 |

[← Previous ID](#)

[Next ID →](#)

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](#)