

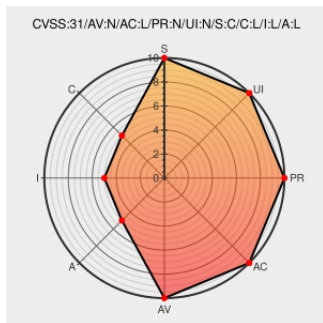


# CVE-2020-11052

Published on: 05/07/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:24 PM UTC

## CVE-2020-11052 - advisory for GHSA-jc8m-cxhj-668x

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

Certain versions of [Sorcery](#) from [Sorcery Project](#) contain the following vulnerability:

In Sorcery before 0.15.0, there is a brute force vulnerability when using password authentication via Sorcery. The brute force protection submodule will prevent a brute force attack for the defined lockout period, but once expired, protection will not be re-enabled until a user or malicious actor logs in successfully. This does not affect users that

do not use the built-in brute force protection submodule, nor users that use permanent account lockout. This has been patched in 0.15.0.

CVE-2020-11052 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: **Sorcery** - Sorcery version < 0.15.0

CVSS3 Score: **9.8 - CRITICAL**

| 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>HIGH</b>            | <b>HIGH</b>         | <b>HIGH</b>         |

CVSS2 Score: **5 - MEDIUM**

| Access Vector          | Access Complexity | Authentication      |
|------------------------|-------------------|---------------------|
| <b>NETWORK</b>         | <b>LOW</b>        | <b>NONE</b>         |
| Confidentiality Impact | Integrity Impact  | Availability Impact |
| <b>PARTIAL</b>         | <b>NONE</b>       | <b>NONE</b>         |

CVE References

Description

Fix brute force vuln due to callbacks not being ran by athix · Pull Request #235 · Sorcery/sorcery · GitHub

Tags

Patch

Third Party Advisory

github.com

text/html

Link

 [MISC github.com/Sorcery/sorcery/pull/235](https://github.com/Sorcery/sorcery/pull/235)

Description

Fix brute force vuln due to callbacks not being ran (#235) · Sorcery/sorcery@0f116d2 · GitHub

Tags

Patch

Third Party Advisory

github.com

text/html

Link

 [MISC github.com/Sorcery/sorcery/commit/0f116d223826895a73b12492f17486e5d54ab7a7](https://github.com/Sorcery/sorcery/commit/0f116d223826895a73b12492f17486e5d54ab7a7)

Description

Brute Force Vulnerability · Advisory · Sorcery/sorcery · GitHub

Tags

Third Party Advisory

github.com

text/html

Link

 [CONFIRM github.com/Sorcery/sorcery/security/advisories/GHSA-jc8m-cxhj-668x](https://github.com/Sorcery/sorcery/security/advisories/GHSA-jc8m-cxhj-668x)

Description

brute force vulnerability · Issue #231 · Sorcery/sorcery · GitHub

Tags

Third Party Advisory

github.com

text/html

Link

 [MISC github.com/Sorcery/sorcery/issues/231](https://github.com/Sorcery/sorcery/issues/231)

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="#">Sorcery Project</a> | <a href="#">Sorcery</a> | All     | All    | All     | All      |
| Application | <a href="#">Sorcery Project</a> | <a href="#">Sorcery</a> | All     | All    | All     | All      |

cpe:2.3:a:sorcery\_project:sorcery:\*\*\*\*\*:ruby:\*\*\*:

cpe:2.3:a:sorcery\_project:sorcery:\*\*\*\*\*:ruby:\*\*\*:

No vendor comments have been submitted for this CVE

← 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](#)