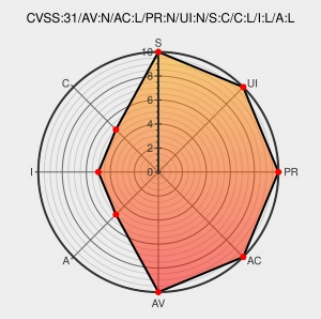
CVE-2020-11052

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
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Fix brute force vuln due to callbacks not being ran by athix · Pull Request #235 · Sorcery/sorcery · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/Sorcery/sorcery/pull/235
Fix brute force vuln due to callbacks not being ran (#235) · Sorcery/sorcery@0f116d2 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/Sorcery/sorcery/commit/0f116d223826895a73b12492f17486e5d54ab7a7
Brute Force Vulnerability · Advisory · Sorcery/sorcery · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/Sorcery/sorcery/security/advisories/GHSA-jc8m-cxhj-668x
brute force vulnerability · Issue #231 · Sorcery/sorcery · GitHub	Third Party Advisory github.com text/html	MISC github.com/Sorcery/sorcery/issues/231

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sorcery Project	Sorcery	All	All	All	All
Application	Sorcery Project	Sorcery	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→