

 Search by package name c

Server-side Request Forgery (SSRF)

Affecting [github.com/hoppscotch/proxyscotch](#) package,
versions <1.0.0

INTRODUCED: 29 MAR 2022 [CVE-2022-25850](#) ⓘ [CWE-918](#) ⓘ

Share ▾

FIRST ADDED BY SNYK

How to fix?

Upgrade [github.com/hoppscotch/proxyscotch](#) to version 1.0.0 or higher.

Overview

Affected versions of this package are vulnerable to Server-side Request Forgery (SSRF) when interceptor mode is set to proxy. It occurs when an HTTP request is made by a backend server to an untrusted URL submitted by a user. It leads to a leakage of sensitive information from the server.

References

- [GitHub Commit](#)



Snyk CVSS

Exploit Maturity	Proof of concept ⓘ
Attack Complexity	Low ⓘ
Confidentiality	HIGH ⓘ
See more	

> NVD

7.5 HIGH

Do your applications use this vulnerable package?

In a few clicks we can analyze your entire application and see what components are vulnerable in your application, and suggest you quick fixes.

Test your applications

SnykSNYK-GOLANG-
ID GITHUBCOMHOPPSCTCHPROX
2425228

2435220

Published 31 Mar 2022

Disclosed 29 Mar 2022

Credit Yadhu Krishna M

Report a new vulnerability

Found a mistake?

PRODUCT

Snyk Open Source

Snyk Code

Snyk Container

Snyk Infrastructure as Code

Test with Github

Test with CLI

RESOURCES

Vulnerability DB

Documentation

Disclosed Vulnerabilities

Blog

FAQs

COMPANY

About

Jobs

Contact

Policies

Do Not Sell My Personal Information

CONTACT US

Support

[Report a new vuln](#)

[Press Kit](#)

[Events](#)

FIND US ONLINE

TRACK OUR DEVELOPMENT



Join the >>
community

© 2022 Snyk Limited

Registered in England and Wales. Company number: 09677925

Registered address: Highlands House, Basingstoke Road, Spencers Wood, Reading, Berkshire, RG7 1NT.