



CVE-2022-25850

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-25850
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-01 16:15:00 UTC
Updated	2022-05-11 17:41:00 UTC
Description	The package github.com/hoppscotch/proxyscotch before 1.0.0 are vulnerable to Server-side Request Forgery (SSRF) when

Risk And Classification

Problem Types: CWE-918

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Proxyscotch Project	Proxyscotch	All	All	All	All

References

Reference	Source	Link
feat: ability to have a blacklist of target urls for proxy to make ca... · hoppscotch/proxyscotch@de67380 · GitHub	MISC	github.com
Server-side Request Forgery (SSRF) in github.com/hoppscotch/proxyscotch CVE-2022-25850 Snyk	MISC	snyk.io
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Yadhu Krishna M

There are currently no legacy QID mappings associated with this CVE.

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report