



CVE-2023-36474

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-36474
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-28 22:15:00 UTC
Updated	2023-07-07 14:54:00 UTC
Description	Interactsh is an open-source tool for detecting out-of-band interactions. Domains configured with interactsh server prior to v

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Projectdiscovery	Interactsh	All	All	All	All

References

Reference	Source	Link	Ta
deprecate default cname entry · Issue #136 · projectdiscovery/interactsh · GitHub	MISC	github.com	
Hostile Subdomain Takeover using Heroku/Github/Desk + more - Detectify Labs	MISC	labs.detectify.com	
Interactsh server < 1.0.0 Subdomain Takeover · Advisory · projectdiscovery/interactsh · GitHub	MISC	github.com	
Making app CNAME optional by Mzack9999 · Pull Request #155 · projectdiscovery/interactsh · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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](#)