



CVE-2023-46117

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

Summary

CVE	CVE-2023-46117
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-20 19:15:00 UTC
Updated	2023-10-28 03:48:00 UTC
Description	reconFTW is a tool designed to perform automated recon on a target domain by running the best set of tools to perform sca

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Six2dez	Reconftw	All	All	All	All

References

Reference	Source
Inadequate validation of retrieved subdomains may lead to a Remote Code Execution (RCE) · Advisory · six2dez/reconftw · GitHub	MISC
fix regex · six2dez/reconftw@e639de3 · GitHub	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

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