CVE-2020-7734

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2020-7734
State	PUBLIC
Assigner	report@snyk.io
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-22 08:15:00 UTC
Updated	2020-09-30 16:04:00 UTC
Description	All versions of package cabot are vulnerable to Cross-site Scripting (XSS) via the Endpoint column.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arachnys	Cabot	All	All	All	All

References

Reference	Source	Li
Cross-site Scripting (XSS) in cabot | Snyk	CONFIRM	sn
Its Me AnonArtist	CONFIRM	its
Cabot 0.11.12 - Persistent Cross-Site Scripting - Multiple webapps Exploit	CONFIRM	ww
Security Fix for Stored Cross-site Scripting (XSS) - huntr.dev by huntr-helper · Pull Request #694 · arachnys/cabot · GitHub	CONFIRM	git
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nv

Vendor Comments And Credit

Discovery Credit

LEGACY: anonartistnot0

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

Free CVE JSON API cve.report/api

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