



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	Link
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	wv
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	wv
NVD vulnerability detail	NVD	nv

Vendor Comments And Credit

Discovery Credit

LEGACY: anonartistnot0

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)