



CVE-2022-34754

Published on: Not Yet Published

Last Modified on: 07/22/2022 10:27:00 PM UTC

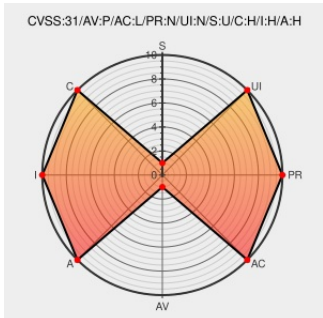
CVE-2022-34754

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of **Acti9 Powertag Link C A9xelc10-a** from **Schneider-electric** contain the following vulnerability:

A CWE-269: Improper Privilege Management vulnerability exists that could allow elevated functionality when guessing credentials. Affected Products: Acti9 PowerTag Link C (A9XELC10-A) (V1.7.5 and prior), Acti9 PowerTag Link C (A9XELC10-B) (V2.12.0 and prior)

CVE-2022-34754 has been assigned by cybersecurity@schneider-electric.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Schneider Electric - Acti9 PowerTag Link C** version < V1.7.5

Affected Vendor/Software: **Schneider Electric - Acti9 PowerTag Link C** version < V2.12.0

CVSS3 Score: **6.8 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
	download.schneider-electric.com application/pdf Inactive Link Not Archived	MISC download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-193-03&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2022-193-03_Acti9_PowerTag_Link_C_Security_Notification.pdf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

591232 Schneider Electric Acti9 PowerTag Link C Improper Privilege Management Vulnerability (SEVD-2022-193-03)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 	Schneider-electric	Acti9 Powertag Link C A9xelc10-a	-	All	All	All
Operating System	Schneider-electric	Acti9 Powertag Link C A9xelc10-a Firmware	All	All	All	All
Hardware 	Schneider-electric	Acti9 Powertag Link C A9xelc10-b	-	All	All	All
Operating System	Schneider-electric	Acti9 Powertag Link C A9xelc10-b Firmware	All	All	All	All
cpe:2.3:h:schneider-electric:acti9_powertag_link_c_(a9xelc10-a):-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:schneider-electric:acti9_powertag_link_c_(a9xelc10-a)_firmware::~~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:h:schneider-electric:acti9_powertag_link_c_(a9xelc10-b):-:~::~~::~~::~~::~~::~~::~~:::						
cpe:2.3:o:schneider-electric:acti9_powertag_link_c_(a9xelc10-b)_firmware::~~::~~::~~::~~::~~::~~::~~:::						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-34754 : A CWE-269: Improper Privilege Management vulnerability exists that could allow elevated functional... twitter.com/i/web/status/1...	2022-07-13 21:17:08
 @threatmeter	CVE-2022-34754 Schneider Electric Acti9 PowerTag Link C up to 1.7.5/2.12.0 privileges management (SEVD-2022-193-0... twitter.com/i/web/status/1...	2022-07-14 07:50:45
 @ColorTokensInc	Emerging Vulnerability Found CVE-2022-34754 - A CWE-269: Improper Privilege Management vulnerability exists that co... twitter.com/i/web/status/1...	2022-07-14 07:50:52
 /r/netcve	CVE-2022-34754	2022-07-13 21:38:59

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2023   |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)