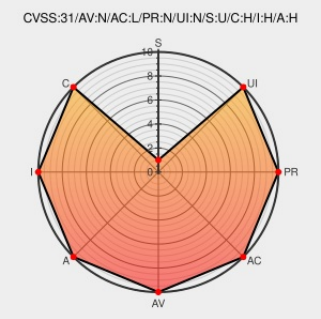
CVE-2020-7548

Published on: 12/01/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:54 PM UTC

CVE-2020-7548

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Acti9 Powertag Link from Schneider-electric contain the following vulnerability:

A CWE-330 - Use of Insufficiently Random Values vulnerability exists in Smartlink, PowerTag, and Wiser Series Gateways (see security notification for version information) that could allow unauthorized users to login.

CVE-2020-7548 has been assigned by cybersecurity@schneider-electric.com to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Notification - Smartlink, PowerTag, and Wiser Series Gateways | Schneider Electric	Patch, Vendor Advisory, www.se.com, text/html	MISC www.se.com/ww/en/download/document/SEVD-2020-287-03/

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

591404 Schneider Electric Smartlink, PowerTag and Wiser Series Gateways Use of Insufficiently Random Values Vulnerability (SEVD-2020-287-03)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Schneider-electric	Acti9 Powertag Link	-	All	All	All
Hardware	Schneider-electric	Acti9 Powertag Link	-	All	All	All
Operating System	Schneider-electric	Acti9 Powertag Link Firmware	All	All	All	All
Operating System	Schneider-electric	Acti9 Powertag Link Firmware	All	All	All	All
Hardware	Schneider-electric	Acti9 Powertag Link Hd	-	All	All	All
Hardware	Schneider-electric	Acti9 Powertag Link Hd	-	All	All	All
Operating System	Schneider-electric	Acti9 Powertag Link Hd Firmware	All	All	All	All
Operating System	Schneider-electric	Acti9 Powertag Link Hd Firmware	All	All	All	All
Hardware	Schneider-electric	Acti9 Smartlink El B	-	All	All	All
Hardware	Schneider-electric	Acti9 Smartlink El B	-	All	All	All
Operating System	Schneider-electric	Acti9 Smartlink El B Firmware	All	All	All	All
Operating System	Schneider-electric	Acti9 Smartlink El B Firmware	All	All	All	All
Hardware	Schneider-electric	Acti9 Smartlink Si B	-	All	All	All
Hardware	Schneider-electric	Acti9 Smartlink Si B	-	All	All	All
Operating System	Schneider-electric	Acti9 Smartlink Si B Firmware	All	All	All	All
Operating System	Schneider-electric	Acti9 Smartlink Si B Firmware	All	All	All	All
Hardware	Schneider-electric	Acti9 Smartlink Si D	-	All	All	All
Hardware	Schneider-electric	Acti9 Smartlink Si D	-	All	All	All
Operating System	Schneider-electric	Acti9 Smartlink Si D Firmware	All	All	All	All
Operating	Schneider-electric	Acti9 Smartlink Si D Firmware	All	All	All	All

System						
Hardware	Schneider-electric	Wiser Energy	-	All	All	All
Hardware	Schneider-electric	Wiser Energy	-	All	All	All
Operating System	Schneider-electric	Wiser Energy Firmware	All	All	All	All
Operating System	Schneider-electric	Wiser Energy Firmware	All	All	All	All
Hardware	Schneider-electric	Wiser Link	-	All	All	All
Hardware	Schneider-electric	Wiser Link	-	All	All	All
Operating System	Schneider-electric	Wiser Link Firmware	All	All	All	All
Operating System	Schneider-electric	Wiser Link Firmware	All	All	All	All

cpe:2.3:h:schneider-electric:acti9_powertag_link:-:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:acti9_powertag_link:-:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:acti9_powertag_link_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:acti9_powertag_link_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:acti9_powertag_link_hd:-:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:acti9_powertag_link_hd:-:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:acti9_powertag_link_hd_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:acti9_powertag_link_hd_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:acti9_smartlink_el_b:-:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:acti9_smartlink_el_b:-:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:acti9_smartlink_el_b_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:acti9_smartlink_el_b_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:acti9_smartlink_si_b:-:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:acti9_smartlink_si_b:-:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:acti9_smartlink_si_b_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:acti9_smartlink_si_b_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:acti9_smartlink_si_d:-:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:acti9_smartlink_si_d:-:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:acti9_smartlink_si_d_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:acti9_smartlink_si_d_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:wiser_energy:-:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:wiser_energy:-:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:wiser_energy_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:wiser_energy_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:wiser_link:-:*:*:*:*:*:*:*:

cpe:2.3:h:schneider-electric:wiser_link:-:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:wiser_link_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:schneider-electric:wiser_link_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→