SSA-723417: Multiple Vulnerabilities in SCALANCE W1750D

Publication Date: 2021-05-11
Last Update: 2021-05-11
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Siemens SCALANCE W1750D is a brand-labeled device. Aruba has released a related security advisory ARUBA-PSA-2021-007 disclosing vulnerabilities in its Aruba Instant product line.

Siemens is preparing updates and recommends countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1750D: All versions < V8.7.0	Update to V8.7.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109782770
SCALANCE W1750D: V8.7.0 only affected by CVE-2020-24635, CVE-2020-24636, CVE-2021-25145, CVE-2021-25146, CVE-2021-25155, CVE-2021-25156, CVE-2021-25157, CVE-2021-25158, CVE-2021-25159, CVE-2021-25160, CVE-2021-25161, CVE-2021-25162	See recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Block access to the Aruba Instant device IP address on port UDP/8211 from all untrusted users
- Block access to the Aruba Instant Command Line Interface from all untrusted users
- Block access to the Aruba Instant Web Management Interface from all untrusted users

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

The SCALANCE W1750D controller-based Direct Access Points support radio transmission according to the latest IWLAN standard IEEE 802.11ac Wave 2.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2019-5317

A local authentication bypass vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-5319

A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2020-24635

A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2020-24636

A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2021-25143

A remote Denial of Service (DoS) vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-25144

A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’)

Vulnerability CVE-2021-25145

A remote unauthorized disclosure of information vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-25146

A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	7.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command (‘Command Injection’)

Vulnerability CVE-2021-25148

A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-25149

A remote buffer overflow vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’)

Vulnerability CVE-2021-25150

A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command (‘Command Injection’)

Vulnerability CVE-2021-25155

A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-25156

A remote arbitrary directory create vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-25157

A remote arbitrary file read vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-25158

A remote arbitrary file read vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization (‘Race Condition’)

Vulnerability CVE-2021-25159

A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-25160

A remote arbitrary file modification vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N/E:P/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2021-25161

A remote cross-site scripting (xss) vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:U/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)

Vulnerability CVE-2021-25162

A remote execution of arbitrary commands vulnerability was discovered in some Aruba Instant Access Point (IAP).

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command (‘Command Injection’)

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2021-05-11): Publication Date

TERMS OF USE