**SSA-723417: Multiple Vulnerabilities in SCALANCE W1750D**

**Publication Date:** 2021-05-11  
**Last Update:** 2021-10-12  
**Current Version:** V1.2  
**CVSS v3.1 Base Score:** 9.8

**SUMMARY**

The Scalance W1750D device contains multiple vulnerabilities that could allow an attacker to inject commands or trigger buffer overflows.

Siemens has released updates for the affected products and recommends to update to the latest versions.

**AFFECTED PRODUCTS AND SOLUTION**

<table>
<thead>
<tr>
<th>Affected Product and Versions</th>
<th>Remediation</th>
</tr>
</thead>
</table>
| **SCALANCE W1750D:**  
  All versions < V8.7.0 | Update to V8.7.0 or later version  
| **SCALANCE W1750D:**  
  All versions >= V8.7.0 and < V8.7.1.3  
  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, CVE-2021-34617, CVE-2021-34618 | Update to V8.7.1.3 or later version  
  https://support.industry.siemens.com/cs/de/en/view/109802805/ |

**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](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](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
- **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
- **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
- **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
- **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
- 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
- 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
- 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
- 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
- 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
- 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
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
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
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
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
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
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
- **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
- **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
- **CWE**: CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2021-34617

A vulnerability in the captive portal of Aruba Instant could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against another user of the portal. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface.

- **CVSS v3.1 Base Score**: 6.1
- **CWE**: CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)

Vulnerability CVE-2021-34618

An unauthenticated Denial of Service vulnerability exists in affected Aruba Instant access points. Exploitation of this vulnerability is only possible via direct ethernet connection to the access point. This vulnerability can be exploited through the LLDP protocol and successful exploitation results in the unavailability of the affected access point due to resource exhaustion.

- **CVSS v3.1 Base Score**: 6.5
- **CWE**: CWE-400: Uncontrolled Resource Consumption

**ADDITIONAL INFORMATION**

Siemens SCALANCE W1750D is a brand-labeled device from Aruba. For more information regarding the listed vulnerabilities see the Aruba security advisory ARUBA-PSA-2021-007: https://www.arubanetworks.com
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
V1.1 (2021-08-10): Added CVE-2021-34617 and CVE-2021-34618 from updated Aruba Advisory
V1.2 (2021-10-12): Added solution for SCALANCE W1750D

**TERMS OF USE**

Siemens Security Advisories are subject to the terms and conditions contained in Siemens’ underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter “License Terms”). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens’ Global Website (https://www.siemens.com/terms_of_use, hereinafter “Terms of Use”), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.