SSA-716164: Multiple Vulnerabilities in Scalance W1750D

Publication Date: 2024-02-13
Last Update: 2024-04-09
Current Version: V1.1
CVSS v3.1 Base Score: 9.8

SUMMARY

The SCALANCE W1750D devices contain multiple vulnerabilities that could allow an attacker to inject commands or exploit buffer overflow vulnerabilities which could lead to sensitive information disclosure, unauthenticated denial of service or unauthenticated remote code execution.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1750D (JP) (6GK5750-2HX01-1AD0): All versions < V8.10.0.9 affected by all CVEs	Update to V8.10.0.9 or later version The update is available upon request from customer support See further recommendations from section Workarounds and Mitigations
SCALANCE W1750D (ROW) (6GK5750-2HX01-1AA0): All versions < V8.10.0.9 affected by all CVEs	Update to V8.10.0.9 or later version The update is available upon request from customer support See further recommendations from section Workarounds and Mitigations
SCALANCE W1750D (USA) (6GK5750-2HX01-1AB0): All versions < V8.10.0.9 affected by all CVEs	Update to V8.10.0.9 or later version The update is available upon request from customer support See further 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:

- CVE-2023-45614, CVE-2023-45615, CVE-2023-45616, CVE-2023-45617, CVE-2023-45618, CVE-2023-45619, CVE-2023-45620, CVE-2023-45621, CVE-2023-45622, CVE-2023-45623, CVE-2023-45624: Enabling cluster-security via the cluster-security command will prevent the vulnerabilities from being exploited
- CVE-2023-45625, CVE-2023-45626, CVE-2023-45627: The CLI and web-based management interfaces should be restricted to a dedicated layer 2 segment/VLAN and/or controlled by firewall policies at layer 3 and above

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

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

SCALANCE W1750D is an Access Point that supports IEEE 802.11ac standards for high-performance WLAN, and is equipped with two dual-band radios, which can provide access and monitor the network simultaneously.

VULNERABILITY DESCRIPTION

This chapter describes all vulnerabilities (CVE-IDs) addressed in this security advisory. Wherever applicable, it also documents the product-specific impact of the individual vulnerabilities.

Vulnerability CVE-2023-45614

There are buffer overflow vulnerabilities in the underlying CLI service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.

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:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2023-45615

There are buffer overflow vulnerabilities in the underlying CLI service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities result in the ability to execute arbitrary code as a privileged user on the underlying operating system.

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:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2023-45616

There is a buffer overflow vulnerability in the underlying AirWave client service that could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's access point management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system.

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:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2023-45617

There are arbitrary file deletion vulnerabilities in the CLI service accessed by PAPI (Aruba's access point management protocol). Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files on the underlying operating system, which could lead to the ability to interrupt normal operation and impact the integrity of the access point.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-45618

There are arbitrary file deletion vulnerabilities in the AirWave client service accessed by PAPI (Aruba's access point management protocol). Successful exploitation of these vulnerabilities result in the ability to delete arbitrary files on the underlying operating system, which could lead to the ability to interrupt normal operation and impact the integrity of the access point.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-45619

There is an arbitrary file deletion vulnerability in the RSSI service accessed by PAPI (Aruba's access point management protocol). Successful exploitation of this vulnerability results in the ability to delete arbitrary files on the underlying operating system, which could lead to the ability to interrupt normal operation and impact the integrity of the access point.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-45620

Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the CLI service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to interrupt the normal operation of the affected access point.

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:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-45621

Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the CLI service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to interrupt the normal operation of the affected access point.

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:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-45622

Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the BLE daemon service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to interrupt the normal operation of the affected access point.

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:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-45623

Unauthenticated Denial-of-Service (DoS) vulnerabilities exist in the Wi-Fi Uplink service accessed via the PAPI protocol. Successful exploitation of these vulnerabilities result in the ability to interrupt the normal operation of the affected access point.

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:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-45624

An unauthenticated Denial-of-Service (DoS) vulnerability exists in the soft ap daemon accessed via the PAPI protocol. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point.

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:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-45625

Multiple authenticated command injection vulnerabilities exist in the command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.

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:O/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2023-45626

An authenticated vulnerability has been identified allowing an attacker to effectively establish highly privileged persistent arbitrary code execution across boot cycles.

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:O/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2023-45627

An authenticated Denial-of-Service (DoS) vulnerability exists in the CLI service. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected access point.

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

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-2023-017: https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2023-017.txt.

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 (2024-02-13): Publication Date
V1.1 (2024-04-09): Added fix for SCALANCE W1750D family

TERMS OF USE