SSA-506569: Multiple Vulnerabilities in SCALANCE W1750D

Publication Date: 2022-11-08
Last Update: 2022-11-08
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

The SCALANCE W1750D device contains multiple vulnerabilities that could allow an attacker to inject commands or exploit buffer overflow vulnerabilities which could lead to denial of service, unauthenticated remote code execution or stored XSS.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1750D (JP) (6GK5750-2HX01-1AD0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W1750D (ROW) (6GK5750-2HX01-1AA0): All versions	Currently no fix is available See recommendations from section Workarounds and Mitigations
SCALANCE W1750D (USA) (6GK5750-2HX01-1AB0): All versions	Currently no fix is available 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:

- CVE-2022-37885, CVE-2022-37886, CVE-2022-37887, CVE-2022-37888, CVE-2022-37889: Enable CPSec via the cluster-security command
- CVE-2022-37890, CVE-2022-37891, CVE-2022-37892, CVE-2022-37895, CVE-2022-37896: Restrict the web-based management interface to a dedicated layer 2 segment/VLAN and/or control the interface by firewall policies at layer 3 and above
- CVE-2022-37893: Restrict the command line interface to a dedicated layer 2 segment/VLAN and/or control the interface by firewall policies at layer 3 and above

Please follow the General Security Recommendations.

 © Siemens 2022

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 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-2002-20001

The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys, and trigger expensive server-side DHE modular-exponentiation calculations, aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE, and the server must be configured to allow DHE. (ATLWL-266)

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:T/RC:C
CWE	CWE-400: Uncontrolled Resource Consumption

Vulnerability CVE-2022-37885

A buffer overflow vulnerability in an underlying service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI UDP port (8211). (ATLWL-253)

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:T/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-37886

A buffer overflow vulnerability in an underlying service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI UDP port (8211). (ATLWL-254)

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:T/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-37887

A buffer overflow vulnerability in an underlying service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI UDP port (8211). (ATLWL-299)

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:T/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-37888

A buffer overflow vulnerability in an underlying service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI UDP port (8211). (ATLWL-300)

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:T/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-37889

A buffer overflow vulnerability in an underlying service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI UDP port (8211). (ATLWL-302)

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:T/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-37890

An unauthenticated buffer overflow vulnerability exists within the web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system. (ATLWL-102)

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:T/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-37891

An unauthenticated buffer overflow vulnerability exists within the web management interface. Successful exploitation results in the execution of arbitrary commands on the underlying operating system. (ATLWL-268)

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:T/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2022-37892

A vulnerability in the web management interface could allow an unauthenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. (ATLWL-168)

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N/E:P/RL:T/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Vulnerability CVE-2022-37893

An authenticated command injection vulnerability exists in the command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. (ATLWL-97)

CVSS v3.1 Base Score	7.8
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C
CWE	CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection')

Vulnerability CVE-2022-37894

An unauthenticated denial of service (DoS) vulnerability exists in the handling of certain SSID strings. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected Access Point. (ATLWL-242)

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

Vulnerability CVE-2022-37895

An authenticated denial of service (DoS) vulnerability exists in the web management interface. Successful exploitation of this vulnerability results in the ability to interrupt the normal operation of the affected Access Point. (ATLWL-248)

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:N/A:H/E:P/RL:T/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2022-37896

A vulnerability in the web management interface could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface. (ATLWL-234)

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:T/RC:C
CWE	CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

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-2022-014 https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2022-014.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 (2022-11-08): Publication Date

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.