SSA-280624: Multiple Vulnerabilities in SCALANCE W1750D

Publication Date: 2021-10-12
Last Update: 2022-10-11
Current Version: V1.1
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 multiple buffer overflow vulnerabilities that could lead to denial of service or unauthenticated remote code execution.

Siemens has released updates for the SCALANCE W1750D and recommends to update to the latest version. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1750D: All versions < V8.7.1.3	Update to V8.7.1.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109802805/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1750D: All versions >= 8.7.1.9 only affected by CVE-2019-5318	Currently no fix is planned See recommendations from section Workarounds and Mitigations
SCALANCE W1750D: All versions >= V8.7.1.3 < V8.7.1.9 only affected by CVE-2019-5318, CVE-2021-37717, CVE-2021-37718, CVE-2021-37719, CVE-2021-37720, CVE-2021-37721, CVE-2021-37722, CVE-2021-37728	Update to V8.7.1.9 or later version https://support.industry.siemens.com/cs/ww/en/view/109813747/ 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:

- Block access to the ArubaOS Command Line Interface from all untrusted users
- Block access to the ArubaOS web-based management interface from all untrusted users
- Block access to the Mobility Conductor Command Line Interface from all untrusted users
- Enabling the Enhanced PAPI Security feature where available will prevent exploitation of these vulnerabilities. Please contact TAC for assistance if needed
- Exploitation requires physical access. Controllers in strictly controlled physical environments are at low risk
- In order to minimize the likelihood of an attacker exploiting these vulnerabilities, Aruba recommends that the communication between Controller/Gateways and Access-Points be restricted either by having a dedicated layer 2 segment/VLAN or, if Controller/Gateways and Access-Points cross layer 3 boundaries, to have firewall policies restricting the communication of these authorized devices. Also, enabling the Enhanced PAPI Security feature will prevent the PAPI-specific vulnerabilities above from being exploited. Contact Aruba Support for configuration assistance

- The RAPConsole or Local Debug homepage can be reached by users in a split or bridge role. This can be prevented by configuring an ACL to restrict access to the Local Debug (LD) homepage which effectively prevents this issue. Instructions on how to implement this ACL can be found at https://www.arubanetworks.com/techdocs/ArubaOS_86_Web_Help/Content/arubaos-solutions/rap/rest-local-deb.htm

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 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-2019-5318

The web interface for RAPConsole lacks Anti-CSRF protections in place for state-changing operations. This can potentially be exploited by an attacker to reboot the affected device if the attacker can convince a user to visit a specially-crafted web page.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

Vulnerability CVE-2021-37716

There are multiple buffer overflow vulnerabilities that could lead to unauthenticated remote code execution by sending especially crafted packets destined to the PAPI (Aruba Networks AP management protocol) UDP port (8211) of devices running ArubaOS. This may potentially allow for denial-of-service attacks and/or remote code execution in 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-2021-37717

Authenticated command injection vulnerabilities exist in the ArubaOS web-based management user interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.

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-2021-37718

Authenticated command injection vulnerabilities exist in the ArubaOS web-based management user interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.

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-2021-37719

A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.

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-2021-37720

Authenticated command injection vulnerabilities exist in the ArubaOS 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. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.

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-2021-37721

Authenticated command injection vulnerabilities exist in the ArubaOS 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. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.

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-2021-37722

Authenticated command injection vulnerabilities exist in the ArubaOS 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. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.

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-2021-37723

Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. These particular vulnerabilities are only present in instances of the Mobility Conductor. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the Mobility Conductor running ArubaOS.

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-2021-37724

Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. These particular vulnerabilities are only present in instances of the Mobility Conductor. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the Mobility Conductor running ArubaOS.

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-2021-37725

A vulnerability in the web-based management interface of ArubaOS could allow an unauthenticated remote attacker to conduct a Cross-Site Request Forgery (CSRF) attack against a vulnerable system. A successful exploit would consist of an attacker persuading an authorized user to follow a malicious link, resulting in the deletion of arbitrary files with the privilege level of the targeted user.

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:N/E:P/RL:O/RC:C
CWE	CWE-352: Cross-Site Request Forgery (CSRF)

Vulnerability CVE-2021-37728

Authenticated path traversal vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to impact the integrity of critical files on the underlying operating system. This allows an attacker to impact the availability of the ArubaOS instance and may allow for modification of sensitive data.

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:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2021-37729

An authenticated path traversal vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to impact the integrity of critical files on the underlying operating system. This allows an attacker to impact the availability of the ArubaOS instance and may allow for modification of sensitive data.

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:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2021-37731

An authenticated local path traversal vulnerability exists in the ArubaOS web-based management interface and CLI. This vulnerability only affects physical hardware controllers such as the 9000 series and 7x00 series. Successful exploitation of this vulnerability requires physical access to the controller and results in the ability to impact the integrity and confidentiality of critical files on the underlying operating system. This allows an attacker to impact the availability of the ArubaOS instance and may allow for modification or disclosure of sensitive data.

CVSS v3.1 Base Score	6.1
CVSS Vector	CVSS:3.1/AV:P/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-311: Missing Encryption of Sensitive Data

Vulnerability CVE-2021-37733

An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to read arbitrary files on the underlying operating system, including sensitive system files.

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:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

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-2021-016.

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 (2021-10-12): Publication Date
V1.1 (2022-10-11): Updated the affected product table with SCALANCE W1750D version V8.7.1.9

TERMS OF USE