SSA-917476: Multiple Vulnerabilities in SCALANCE W1750D

Publication Date: 2021-11-09
Last Update: 2021-11-09
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 execute code on the affected device(s), read arbitrary files, or create a denial-of-service condition.

Siemens has released an update for the SCALANCE W1750D and recommends to update to the latest version. Siemens is preparing further 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: All versions < V8.7.1.3	Update to V8.7.1.3 or later version https://support.industry.siemens.com/cs/de/en/view/109802805/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1750D: All versions >= V8.7.1.3 only affected by CVE-2021-37727, CVE-2021-37730, CVE-2021-37734	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 Command Line Interface from all untrusted users
- Block access to the Aruba Instant web-based management 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
- Block access for Aruba Instant device on port UDP/8211 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-2021-37726

A remote buffer overflow vulnerability was discovered in HPE Aruba Instant (IAP). Successful exploitation could allow for unauthenticated remote code execution, potentially resulting in the execution of arbitrary code as a privileged user on the underlying 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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2021-37727

A remote arbitrary command execution vulnerability was discovered in HPE Aruba Instant (IAP) command line interface. If exploited, it could result in the ability to execute arbitrary commands as a privileged user on the underlying OS, potentially compromising the 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-2021-37730

A remote arbitrary command execution vulnerability was discovered in HPE Aruba Instant (IAP) command line interface. If exploited, it could result in the ability to execute arbitrary commands as a privileged user on the underlying OS, potentially compromising the 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-2021-37732

A remote arbitrary command execution vulnerability was discovered in HPE Aruba Instant (IAP) web-based management user interface. If exploited, it could result in the ability to execute arbitrary commands as a privileged user on the underlying OS, potentially compromising the 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-2021-37734

An authenticated arbitrary file read access vulnerability was discovered in Aruba Instant Access Points. Successful exploitation could lead to an attacker reading any file off the underlying filesystem, including system sensitive 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')

Vulnerability CVE-2021-37735

A remote denial of service vulnerability was discovered in Aruba Instant through the command line interface. If an attacker exploits this, they could create a denial-of-service condition, leading ot a temporary loss of service, until the next reboot.

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:O/RC:C
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-2021-017: https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-017.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 (2021-11-09): Publication Date

TERMS OF USE