SSA-431802: Multiple Vulnerabilities in SCALANCE W1750D

Publication Date: 2020-11-10
Last Update: 2020-11-10
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Siemens SCALANCE W1750D is a brandlabled device. Aruba has released a related security advisory (ARUBA-PSA-2016-004) [0] disclosing vulnerabilities in its Aruba Instant product line. The advisory contains multiple related vulnerabilities that are summarized in CVE-2016-2031.

This advisory is a reminder to customers that the PAPI protocol is not a secure protocol and that some device configurations must be taken to mitigate risks. Although this information was previously disclosed, an impending public disclosure by the Google Security Team (focused on Aruba Instant) will call out the vulnerable details of this protocol and bring it to the attention of the attacker community.

Siemens recommends specific countermeasures until fixes are available.

[0] https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2016-004.txt

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1750D: All versions	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:

- Update to the latest firmware version and find further instructions in the the document “Control Plane Security Best Practices” available at https://support.industry.siemens.com/cs/ww/en/view/109782770/. Depending on network configuration and risk tolerance, no action may be required.

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-2016-2031

Multiple vulnerabilities exists in Aruba Instate before 4.1.3.0 and 4.2.3.1 due to insufficient validation of user-supplied input and insufficient checking of parameters, which could allow a malicious user to bypass security restrictions, obtain sensitive information, perform unauthorized actions and execute arbitrary code.

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

ADDITIONAL INFORMATION

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 (2020-11-10): 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.