SSA-549547: Multiple Vulnerabilites in SCALANCE W1750D

Publication Date: 2019-05-14
Last Update: 2019-05-14
Current Version: V1.0
CVSS v3.0 Base Score: 9.8

SUMMARY

The latest update for SCALANCE W1750D fixes multiple vulnerabilities. The most severe could allow an unauthenticated attacker with access to the web interface of an affected device to execute arbitrary system commands within the underlying operating system.

Siemens has released updates for the affected devices.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1750D: All versions < V8.4.0.1	Update to V8.4.0.1 https://support.industry.siemens.com/cs/us/en/view/109766816/

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict access to the web-based management interface to the internal or VPN network.
- Do not browse other websites and do not click on external links while being authenticated to the administrative web interface.
- Apply appropriate strategies for mitigation.

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), 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 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2018-7084

A command injection vulnerability is present that permits an unauthenticated user with access to the web interface of the affected device to execute arbitrary system commands within the underlying operating system. An attacker could use this ability to copy files, read configuration, write files, delete files, or reboot the device.

The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality, integrity and availability of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-7083

A vulnerability exists in the affected devices that allows an unauthenticated attacker to access core dumps of previously crashed processes through the web interface of the device.

The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-16417

A vulnerability is present which allows an unauthenticated user to retrieve recently cached configuration commands by sending a crafted URL to the web interface of an affected device.

The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires no system privileges and no user interaction. An attacker could use the vulnerability to compromise confidentiality of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.5
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-7082

A command injection vulnerability is present in the affected devices that allows an authenticated administrative user to execute arbitrary commands on the underlying operating system.

The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires no user interaction. An attacker could use the vulnerability to compromise confidentiality, integrity and availability of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.2
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-7064

A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected devices that allows an attacker to trick an administrator into clicking a link which could then take administrative actions on the device or expose a session cookie for an administrative session.

The security vulnerability could be exploited by an attacker with network access to the affected system. Successful exploitation requires no system privileges. An attacker could use the vulnerability to compromise confidentiality, integrity and availability of the affected system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	6.4
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:L/E:P/RL:O/RC:C

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 (2019-05-14): 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.