SSA-464260: TLS ROBOT vulnerability in SCALANCE W1750D

Publication Date:	2018-10-09
Last Update:	2018-10-09
Current Version:	V1.0
CVSS v3.0 Base Score:	5.9

SUMMARY

The latest update for SCALANCE W1750D addresses a vulnerability known as *ROBOT Attack*. The vulnerability could allow an attacker to decrypt TLS traffic.

Siemens provides a firmware update and recommends users to update to the new version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1750D: All versions < V8.3.0.1	Update to V8.3.0.1 https://support.industry.siemens.com/cs/us/en/view/109760581

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 interface of the affected devices.

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 3.0 (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-2017-13099

An attacker with network access to affected devices could potentially obtain a TLS session key. If the attacker is able to observe TLS traffic between a legitimate user and the device, then the attacker could decrypt the TLS traffic.

The security vulnerability could be exploited by an attacker who has network access to the web interface of the device and who is able to observe TLS traffic between legitimate users and the web interface of the affected device. The vulnerability could impact the confidentiality of the communication between the affected device and a legitimate user.

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

CVSS v3.0 Base Score	5.9
CVSS Vector	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N/E:U/RL:O/RC:C

ADDITIONAL INFORMATION

Additional information on the TLS ROBOT attack can be found at https://robotattack.org/

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 (2018-10-09):	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.