SSA-120908: Vulnerabilities in Siemens Scalance W-7xx (a/b/g) Product Family

Publication Date 2013-07-31
Last Update 2013-07-31
Current Version V1.0
CVSS Overall Score 7.4

Summary:

Siemens has discovered two potential vulnerabilities in the Siemens Scalance W7xx (IEEE 802.11a/b/g) product family concerning hard-coded SSL certificates for the secured management web interface and an authentication bypass in the command-line based management interface.

Siemens provides an update [1] which fixes both issues.

AFFECTED PRODUCTS

Firmware version < V4.5.4 is affected for the following products supporting IEEE 802.11a/b/g:

- SCALANCE W744-1, W746-1, W747-1
- SCALANCE W744-1PRO, W746-1PRO, W747-1RR
- SCALANCE W784-1, W784-1RR
- SCALANCE W786-1PRO, W786-2PRO, W786-3PRO, W786-2RR
- SCALANCE W788-1PRO, W788-2PRO, W788-1RR, W788-2RR

Alternatively, the affected products may be identified by using their MLFB. Products with the following MLFBs are affected ("x" represents a wild-card symbol):

- 6GK5 7xx-xAxx0-xAx0
- 6GK5 7xx-xBxx0-xAx0
- 6GK5 746-1AA60-4BA0

DESCRIPTION

Scalance W7xx products are wireless communication devices which offer reliability, ruggedness and security for both non-critical communication and process-critical data. The devices are used where mobility of machines and parts is required, or cable installation is too expensive or difficult to implement.

Two vulnerabilities were found in the implementation of the Scalance W7xx firmware. The first vulnerability allows an attacker to perform a man-in-the-middle attack on the SSL-secured management web interface. The second vulnerability allows an attacker to gain complete system access without authentication.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (http://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 1 (CVE-2013-4651)

The devices use a hard-coded SSL certificate for secure communication of their management web interface (HTTPS). It is not possible to change this certificate using the management interfaces. This allows attackers to perform man-in-the-middle (MITM) attacks.

CVSS Base Score 6.6
CVSS Temporal Score 4.9
CVSS Overall Score 4.9 (AV:N/AC:H/Au:N/C:P/I:P/A:C/E:U/RL:OF/RC:C)

Vulnerability 2 (CVE-2013-4652)

The current implementation of the command-line based management interface contains a vulnerability that allows attackers to gain complete system access over the network without authentication. Protocols SSH (port 22/tcp) and Telnet (port 23/tcp) are affected.

CVSS Base Score	10.0
CVSS Temporal Score	7.4
CVSS Overall Score	7.4 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:U/RL:OF/RC:C)

Mitigating factors:

For vulnerability 1, the attacker must have the corresponding private key and appropriate network access to perform a man-in-the-middle attack while an administrator is using the management web interface.

For vulnerability 2, the attacker must have network access to connect to the affected devices.

According to the operational guidelines [2], the management interfaces of Scalance W7xx devices should only be accessible in trusted networks.

SOLUTION

Siemens provides firmware update SCALANCE W7xx V4.5.4 [1] which fixes both vulnerabilities. The update allows users to upload custom SSL certificates for the secured management web interface. To prevent man-in-the-middle attacks, Siemens recommends configuring a custom SSL certificate to secure web communication.

Vulnerability 2 is fixed in the update. If it is not possible to install the firmware update, a workaround for vulnerability 2 is to disable access to the management CLI.

As a general security measure Siemens recommends to protect network access to the management interfaces of Siemens Scalance W7xx devices with appropriate mechanisms. It is advised to follow recommended security practices [4] and to configure the environment according to operational guidelines [2] in order to run the devices in a protected IT environment.

ADDITIONAL RESOURCES

1. The firmware update can be obtained here:
   http://support.automation.siemens.com/WW/view/en/77427398
2. An overview of the operational guidelines for Industrial Security (with the cell protection concept):
   http://www.industry.siemens.com/topics/global/en/industrial-security/Documents/operational_guidelines_industrial_security_en.pdf
3. Information about Industrial Security by Siemens:
   http://www.siemens.com/industrialsecurity
4. Recommended security practices by ICS-CERT:
   http://ics-cert.us-cert.gov/content/recommended-practices
5. For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
   http://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2013-07-31): Publication Date

DISCLAIMER