SSA-176087: Unauthenticated Access to Critical Services in SCALANCE X-200 Switch Family

Publication Date	2013-10-01
Last Update	2013-10-18
Current Version	V1.1
CVSS Overall Score	7.8

Summary:

A potential vulnerability was discovered in the web server authentication of SCALANCE X-200 and X-200IRT switches that might allow attackers to perform administrative operations over the network without authentication. This issue only applies to switches using older firmware versions and has been fixed from firmware V4.5.0 (non-IRT) and V5.1.0 (IRT) on.

Siemens recommends upgrading to the current firmware versions V5.0.1 (non-IRT) [1] and V5.1.2 (IRT) [2].

AFFECTED PRODUCTS

- SCALANCE X-200 switch family with firmware version < V4.5.0
- SCALANCE X-200IRT switch family with firmware version < V5.1.0

All later firmware versions are not affected by the issue. Alternatively, the affected products may be identified by using their MLFB. Products with the following MLFBs may be affected:

- SCALANCE X-200 MLFBs:

6GK5224-0BA00-2AA3	6GK5216-0BA00-2AA3	6GK5212-2BB00-2AA3
6GK5212-2BC00-2AA3	6GK5208-0BA10-2AA3	6GK5206-1BB10-2AA3
6GK5206-1BC10-2AA3	6GK5204-2BB10-2AA3	6GK5204-2BC10-2AA3
6GK5208-0HA10-2AA6	6GK5204-0BA00-2AF2	6GK5208-0BA00-2AF2
6GK5206-1BC00-2AF2	6GK5204-2BC00-2AF2	6GK5204-2BB10-2CA2

- SCALANCE X-200IRT MLFBs:

6GK5201-3JR00-2BA6	6GK5204-0BA00-2BF2	6GK5204-0JA00-2BA6
6GK5202-2JR00-2BA6	6GK5202-2BH00-2BA3	6GK5201-3BH00-2BA3
6GK5200-4AH00-2BA3	6GK5202-2BB00-2BA3	6GK5204-0BA00-2BA3

DESCRIPTION

SCALANCE X-200 switches are used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs). The switches offer a web interface to enable users to change the configuration using a common web browser.

An issue in the web server's authentication of the affected products might allow attackers to perform administrative operations over the network without authentication.

Detailed information about the vulnerability 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 Description (CVE-2013-5944)

The integrated web server of SCALANCE X-200 switches might allow attackers to perform administrative operations over the network without authentication.

CVSS Base Score	10.0
CVSS Temporal Score	7.8
CVSS Overall Score	7.8 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:POC/RL:OF/RC:C)

Mitigating factors:

The attacker must have network access to the device.

SOLUTION

Siemens recommends upgrading to the current SCALANCE X-200 firmware versions V5.0.1 (non-IRT) [1] and V5.1.2 (IRT) [2].

As a general security measure Siemens strongly recommends to protect network access to the management interface of Scalance X switches by appropriate mechanisms. It is advised to follow recommended security practices [5] and to configure the environment according to operational guidelines [3] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENT

Siemens thanks the following people/researchers for their support and efforts:

- Eireann Leverett from IOActive for coordinated disclosure.

ADDITIONAL RESOURCES

[1] The firmware update for SCALANCE X-200 can be obtained here:
http://support.automation.siemens.com/WW/view/en/82142251

[2] The firmware update for SCALANCE X-200IRT can be obtained here:
http://support.automation.siemens.com/WW/view/en/78454417

[3] 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

[4] Information about Industrial Security by Siemens:
http://www.siemens.com/industrialsecurity

[5] Recommended security practices by ICS-CERT:
http://ics-cert.us-cert.gov/content/recommended-practices

[6] 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 (2013-10-01):	Publication Date
V1.1 (2013-10-18):	Changed recommended firmware version for X-200 (non-IRT) to V5.0.1 due to configuration issues of V5.0.0

DISCLAIMER