SSA-850708: Authentication Bypass in SCALANCE X-200 Switch Family

Publication Date	2013-09-11
Last Update	2013-09-11
Current Version	V1.0
CVSS Overall Score	6.5

Summary:

A potential vulnerability was discovered in the web server's authentication of SCALANCE X-200 switches that might allow attackers to hijack web sessions over the network without authentication.

Siemens addresses the issue by a firmware update.

AFFECTED PRODUCTS

- SCALANCE X-200 switch family with firmware version < V5.0.0.

Alternatively, the affected products may be identified by using their MLFB. Products with the following MLFBs are affected:

- 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

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 hijack web sessions 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-2013-5709)

The authentication of the integrated web server of SCALANCE X-200 switches might allow attackers to hijack web sessions over the network without authentication due to insufficient entropy in its random number generator.

CVSS Base Score	8.3
CVSS Temporal Score	6.5
CVSS Overall Score	6.5 (AV:N/AC:M/Au:N/C:P/I:P/A:C/E:POC/RL:OF/RC:C)

Mitigating factors:

The attacker must have network access to the device and a user must be logged in at its web interface.

SOLUTION

Siemens provides SCALANCE X-200 firmware V5.0.0 [1] which fixes the potential vulnerability.

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 [4] and to configure the environment according to operational guidelines [2] 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 can be obtained here:
http://support.automation.siemens.com/WW/view/en/78458674

[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 (2013-09-11): Publication Date

DISCLAIMER