SSA-170686: Vulnerabilities in Siemens Scalance X200 IRT Switch Family

Publication Date	2013-05-24
Last Update	2013-05-27
Current Version	V1.1
CVSS Overall Score	6.3

Summary:

Two vulnerabilities have been reported in the Siemens Scalance X200 IRT switch family concerning a privilege escalation bug in the web interface and an authentication problem in the SNMPv3 implementation. Siemens addresses both vulnerabilities by a firmware upgrade.

AFFECTED PRODUCTS

- SCALANCE X204IRT versions < V5.1.0
- SCALANCE X204IRT PRO versions < V5.1.0
- SCALANCE X202-2IRT versions < V5.1.0
- SCALANCE X202-2P IRT versions < V5.1.0
- SCALANCE X202-2P IRT PRO versions < V5.1.0
- SCALANCE X201-3P IRT versions < V5.1.0
- SCALANCE X201-3P IRT PRO versions < V5.1.0
- SCALANCE X200-4P IRT versions < V5.1.0
- SCALANCE XF204IRT versions < V5.1.0

DESCRIPTION

Scalance X switches are used to connect industrial components like PLCs or HMIs. The switches offer a web interface to enable administrators to change the configuration using a common web browser.

Two vulnerabilities were found in the implementation of the Scalance X200 IRT firmware. The first vulnerability allows an attacker to escalate his privileges within the web interface. The second vulnerability is located in the SNMPv3 implementation, which does not properly check user credentials for SNMPv3 commands.

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-2013-3633)

The user privileges for the web interface are enforced on client side and not properly verified on server side. Therefore, an attacker is able to execute privileged commands using an unprivileged account.

CVSS Base Score	8.0
CVSS Temporal Score	6.3
CVSS Overall Score	6.3 (AV:N/AC:L/Au:S/C:P/I:P/A:C/E:POC/RL:OF/RC:C)

Mitigating factors:

The attacker must have network access to the web interface. According to the operational guidelines for Industrial Security [2], Scalance X switches should only be used inside trusted zones.

Vulnerability 2 (CVE-2013-3634)

The implementation of SNMPv3 does not check the user credentials sufficiently. Therefore, an attacker is able to execute SNMP commands without correct credentials.

CVSS Base Score	7.5
CVSS Temporal Score	5.9
CVSS Overall Score	5.9 (AV:N/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C)

Mitigating factors:

The attacker has to know a valid user name and must have network access to the device.

SOLUTION

Siemens provides firmware update SCALANCE X-200IRT V5.1.0 [1], which fixes both vulnerabilities. If it is not possible to install the firmware update, a workaround for vulnerability 2 is to either disable SNMP or to completely disable any read-write access.

ADDITIONAL RESOURCES

1. The firmware can be obtained here:
   http://support.automation.siemens.com/WW/view/en/73470284
2. An overview of the operational guidelines for Industrial Security (with 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 US-CERT:
   http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html
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 (2013-05-24):	Publication Date
V1.1 (2013-05-27):	Adjusted CVSS Base Score from 6.4 to 7.5 for Vulnerability 2

DISCLAIMER

See: http://www.siemens.com/terms_of_use