SSA-268149: Multiple Security Vulnerabilities in Siemens Scalance S

Publishing Date 2012-04-05
Last Update 2012-04-05
Current Version V1.0
CVSS Overall Score 8.7

Summary:

Two vulnerabilities have been reported in the Siemens Scalance Firewall. Siemens addresses both vulnerabilities by a firmware upgrade.

AFFECTED PRODUCTS

- Scalance S602 V2
- Scalance S612 V2
- Scalance S613 V2

DESCRIPTION

The Scalance S firewall is used to protect trusted industrial networks from untrusted networks. It allows filtering incoming and outgoing network connections in different ways. Scalance S612 and Scalance S613 provide additional security functionality, e.g. VPN tunnels to connect trusted networks ("security cells") in a secure way.

Two vulnerabilities were found in the implementation of the Scalance S firmware. The first vulnerability concerns the web configuration interface of the firewall. This is a web server where no protection against brute-force credential guessing was implemented. Attackers might use this to probe a high number of passwords in a short period of time. Thus, weak passwords can be guessed, allowing the attacker to log into the web interface and change the configuration of the firewall.

The second vulnerability is related to the Profinet DCP protocol, which is an ISO/OSI layer-2 protocol. The Scalance-S DCP protocol stack crashes when a specially crafted DCP frame is received.

Detailed information about the respective 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

The Scalance S web server does not enforce time delays between logon tries. This missing functionality might allow attackers with access to the web server to guess the password with a brute-force attack.

If the administrative password is found, the attacker can manipulate the configuration and gain access to the internal, trusted network.

CVSS Base Score	10
CVSS Temporal Score	8.7
CVSS Overall Score	8.7 (AV:N/AC:L/Au:N/C:C/I:C/A:C/E:H/RL:OF/RC:C)

Vulnerability #2

The Scalance S DCP protocol stack does not handle unexpected input correctly. Certain frames render the firewall unresponsive and established VPN tunnels will be interrupted.

This attack only works from an adjacent network, because DCP is an ISO/OSI layer 2 protocol. Additionally, Scalance S fails in a secure manner, i.e. all access to the internal network is blocked.

CVSS Base Score	6.1
CVSS Temporal Score	4.8
CVSS Overall Score	4.8 (AV:A/AC:L/Au:N/C:N/I:N/A:C/E:POC/RL:OF/RC:C)

Mitigating factors for vulnerability 1:

The attacker has to have network access to the firewall. Using complex passwords and changing them frequently (which is highly recommended in any case) reduces the probability of a successful attack. The maximum length of a password is limited to 32 characters.

Mitigating factors for vulnerability 2:

The attacker has to have access to an adjacent network, because DCP frames are not routed.

SOLUTION

Siemens provides a fix for closing both vulnerabilities. Vulnerability 1 was fixed by limiting the number of login tries during a certain amount of time. Vulnerability 2 was fixed by adjustments in the protocol stack.

Siemens strongly recommends installing the fix as soon as possible.

ACKNOWLEDGEMENT

Siemens thanks Adam Hahn and Manimaran Govindarasu from Iowa State University for coordinated disclosure of the vulnerabilities.

ADDITIONAL RESOURCES

1. The firmware update is published on the following web site:
   http://support.automation.siemens.com/WW/view/en/59869684
2. Information about industrial security by Siemens:
   http://www.siemens.com/industrialsecurity
3. Recommended security practices by US-CERT:
   http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html
4. For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:
   http://www.siemens.com/cert

HISTORY DATA

V1.0 (2012-04-05): Publication Date

DISCLAIMER