SSA-783261: Denial-of-Service vulnerability in Siemens Automation License Manager (ALM)

Publishing Date	2012-12-12
Last Update	2012-12-12
Current Version	V1.0
CVSS Overall Score	4.8

Summary:

A denial-of-service vulnerability has been detected in the Siemens Automation License Manager (ALM), which is used for license management by various Siemens software products. The vulnerability is exploitable within the local subnet and Siemens has addressed this vulnerability by a software update.

AFFECTED PRODUCTS

All Siemens software products that include ALM version >= 4.0 and < 5.2 are affected by the vulnerability. The corresponding ALM version can be determined as described in Section “Solution”.

Products of the following product families are affected:

- SIMATIC (e.g., STEP 7)
- SIMATIC HMI (e.g., WinCC, WinCC flexible)
- SIMATIC PCS 7
- SIMOTION (e.g., Scout)
- SIMATIC NET
- SINAMICS (e.g., Starter)
- SIMOCODE

Note: This list is not exhaustive, so other Siemens software products may also be affected. To find out whether you are affected, please follow the description in Section “Solution”.

DESCRIPTION

ALM centrally manages licenses for various Siemens software products. The products contact ALM either locally or remotely to verify their license using a proprietary protocol. To enable this license verification, ALM listens on TCP port 4410 by default. During installation, this port is enabled for the local subnet by the Windows firewall and requests from other networks are blocked. Internal security tests have detected that specially crafted packets, which are sent to this port, enable a Denial-of-Service attack.

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 Description

Specially crafted packets sent to TCP port 4410 cause memory leaks within the software which eventually leads to a crash of the application due to insufficient resources.

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:

The attacker must have access to the local subnet where ALM is located. During installation, the default setting of the Windows firewall is to block the port used by ALM for all networks except the local subnet. If this setting has not been changed by the administrator, these vulnerabilities cannot be exploited from remote networks. Additionally, communication to this port should be blocked at network borders using appropriate security measures like firewalls.

SOLUTION

Siemens provides a software update for closing all vulnerabilities on [1] (ALM version 5.2). Siemens recommends installing the update as soon as possible. This update can be applied to all systems running ALM Version >= 4.0 and the following Microsoft Windows versions:

- MS Windows XP SP2 or SP3 (32 bit)
- MS Windows Server 2003 SP1 or SP2 Standard Edition w/ or w/o R2 (32 bit)
- MS Windows Server 2008 w/ or w/o SP2 (32 bit)
- MS Windows 7 w/ or w/o SP1 (32 bit)
- MS Windows Server 2008 R2 (64 bit)
- MS Windows 7 w/ or w/o SP1 (64 bit)

The installed ALM version can be determined by the following procedure:

- Start graphical interface of ALM (link on Desktop by default)
- Click on “Help” in the menu bar, then select entry “About …”
- Version is displayed within dialog

ADDITIONAL RESOURCES

1. The software update (ALM version 5.2) is published on the following web site: http://support.automation.siemens.com/WW/view/en/114358
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/advisories

HISTORY DATA

V1.0 (2012-12-12): Publication Date

DISCLAIMER