SIEMENS-SSA-319258: Multiple Security Vulnerabilities in Siemens Automation License Manager (ALM)

Publishing Date 2011-12-16
Last Update 2011-12-16
Current Version V1.1
CVSS Overall Score 7.3

Summary:

Four vulnerabilities have been reported in the Siemens Automation License Manager. Siemens AG will address the vulnerabilities by a software fix. The issued fix will solve all vulnerabilities that exist in version >= 4.0.

AFFECTED SOFTWARE

All Siemens software products that include ALM version >= 4.0 and < 5.1+SP1+Upd2 are affected by vulnerabilities 1-3 (see Section “Vulnerability classification”). Products containing ALM version >= 2.0 and < 5.1+SP1+Upd3 are affected by vulnerability 4. 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, it may be extended in future updates of this advisory. Other Siemens software products may also be affected.

DESCRIPTION

The Siemens Automation License Manager (ALM) is affected by the vulnerabilities. This application centrally manages licenses for various Siemens 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. As received data on this port is not properly sanitized by ALM, it is possible to perform remote code execution and Denial-of-Service attacks. ALM is running with System privileges by default, so one of these vulnerabilities may allow complete system compromise.

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

ALM does not check the length of a field used in various commands sent to the server via the configured port. This vulnerability may lead to remote code execution.

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

Vulnerability #2

In multiple cases ALM does not check the length of fields used in various commands sent to the server via the configured port. These vulnerabilities cause exceptions within the application, which cause the application to quit and enable Denial-of-Service attacks.

CVSS Base Score	6.1
CVSS Temporal Score	5.0
CVSS Overall Score	5.0 (AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C)

Vulnerability #3

ALM does not check the content of a field used a command sent to the server via the configured port. This vulnerability causes a null pointer dereference, which cause the application to quit and enables a Denial-of-Service attack.

CVSS Base Score	6.1
CVSS Temporal Score	5.0
CVSS Overall Score	5.0 (AV:A/AC:L/Au:N/C:N/I:N/A:C/E:F/RL:OF/RC:C)

Vulnerability #4

ALM uses an ActiveX control in its graphical user interface. This control exports a method that allows saving a file to the local hard disk. A malicious web site that the user accesses with Internet Explorer may delete the content of any file on the system that the user is allowed to write to, and create new files.

CVSS Base Score	8.8
CVSS Temporal Score	7.3
CVSS Overall Score	7.3 (AV:N/AC:M/Au:N/C:N/I:C/A:C/E:F/RL:OF/RC:C)

Mitigating factors for vulnerabilities 1, 2, 3:

The attacker has to 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.

If an ALM installation does not work as license server (e.g. floating licenses provided for other systems), remote access should be disabled. The corresponding option can be found in the settings dialog of ALM in tab “Connections”.

Mitigating factors for vulnerability 4:

Do not use Internet Explorer to view local and remote HTML web pages originating from unknown or untrusted sources.

SOLUTION

Siemens provides a fix for closing all vulnerabilities on http://support.automation.siemens.com/WW/view/en/114358 (ALM version 5.1+SP1+Upd3). Siemens strongly recommends installing the fix as soon as possible. This fix 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 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

ACKNOWLEDGEMENT

Siemens thanks

- Luigi Auriemma for discovering the vulnerabilities.
- The Industrial Control Systems Cyber Emergency Response Team (ICS CERT) for coordination efforts.

ADDITIONAL RESOURCES

1. The fix for ALM 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
5. Original vulnerability disclosure: http://www.exploit-db.com/exploits/18165/

HISTORY DATA

V1.1 (2011-12-16): Publication Date

DISCLAIMER

