SSA-284342: Vulnerabilities in Automation License Manager (ALM)

Publication Date 2016-10-12
Last Update 2016-10-12
Current Version V1.0
CVSS v3.0 Base Score 9.1

SUMMARY

The latest update of Automation License Manager (ALM) fixes three vulnerabilities. One of the vulnerabilities could allow a remote attacker to obtain write access to the hard disk.

AFFECTED PRODUCTS

Automation License Manager (ALM): All versions < V5.3 SP3 Update 1

DESCRIPTION

The Automation License Manager (ALM) centrally manages license keys for various Siemens software products. Software products requiring license keys automatically report this requirement to the ALM. When the ALM finds a valid license key for this software, the software can be used in conformity with the end user license agreement.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2016-8563)

Specially crafted packets sent to port 4410/TCP could cause a Denial-of-Service of the ALM service. To recover, the service needs to be restarted manually.

CVSS Base Score 7.5
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C

Vulnerability 2 (CVE-2016-8564)

A SQL Injection vulnerability could allow a remote attacker with access to port 4410/TCP to read and write configuration settings of the Automation License Manager (ALM).

CVSS Base Score 6.5
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N/E:P/RL:O/RC:C

Vulnerability 3 (CVE-2016-8565)

A remote attacker could use specially crafted packets to upload files to the hard disk, create or delete directories or move existing files on the hard disk.

Automation License Manager (ALM) version 5.3 SP3 is not affected by this vulnerability.

CVSS Base Score 9.1
CVSS Vector CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H/E:P/RL:O/RC:C

Mitigating Factors

By default, during the installation the Windows firewall is configured to only allow connections from the local subnet to the ALM default port 4410/TCP and requests from other networks are blocked. Siemens recommends operating the devices only within trusted networks [2].

SOLUTION

Siemens provides Automation License Manager (ALM) version V5.3 SP3 Update 1 [1] which fixes the vulnerabilities. Siemens strongly recommends customers to update to the new version.

As a general security measure Siemens strongly recommends to protect network access to the PC-based automation systems with appropriate mechanisms. It is advised to configure the environment according to our operational guidelines [2] in order to run the devices in a protected IT environment.

ACKNOWLEDGEMENTS

Siemens thanks the following for their support and efforts:

- Sergey Temnikov and Vladimir Dashchenko, Critical Infrastructure Defence Team, Kaspersky Lab for coordinated disclosure of the vulnerabilities.

ADDITIONAL RESOURCES

[1] Automation License Manager (ALM) version V5.3 SP3 Update 1: https://support.industry.siemens.com/cs/ww/en/view/114358

[2] An overview of the operational guidelines for Industrial Security (with the cell protection concept): https://www.siemens.com/cert/operational-guidelines-industrial-security

[3] Information about Industrial Security by Siemens: https://www.siemens.com/industrialsecurity

[4] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT: https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2016-10-12): Publication Date

DISCLAIMER