SSA-476715: Two Vulnerabilities in Automation License Manager

Publication Date: 2023-01-10
Last Update: 2023-03-14
Current Version: V1.1
CVSS v3.1 Base Score: 8.2

SUMMARY

Siemens Automation License Manager contains two vulnerabilities which, when combined, could allow an attacker to modify and rename license files, extract licenses and overwrite arbitrary files on the target system potentially leading to privilege escalation and remote code execution. The affected functionality is not available for remote attackers in the default configuration since version V6.0 SP2 of Automation License Manager.

Siemens has released an update for Automation License Manager V6 and recommends to update to the latest version. Siemens recommends specific countermeasures for products where updates are not, or not yet available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Automation License Manager V5: All versions	Currently no fix is planned See recommendations from section Workarounds and Mitigations
Automation License Manager V6: All versions < V6.0 SP9 Upd4	Update to V6.0 SP9 Upd4 or later version https://support.industry.siemens.com/cs/ww/en/view/114358/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- If remote connections are needed, limit remote access to port 4410/tcp to trusted systems only
- If no remote connections are needed, disable “Allow Remote Connections” on the Automation License Manager settings menu (default since version V6.0 SP2)

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens’ operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals. Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT 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.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://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.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2022-43513

The affected components allow to rename license files with user chosen input without authentication. This could allow an unauthenticated remote attacker to rename and move files as SYSTEM user.

CVSS v3.1 Base Score	8.2
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-73: External Control of File Name or Path

Vulnerability CVE-2022-43514

The affected component does not correctly validate the root path on folder related operations, allowing to modify files and folders outside the intended root directory. This could allow an unauthenticated remote attacker to execute file operations of files outside of the specified root folder. Chained with CVE-2022-43513 this could allow Remote Code Execution.

CVSS v3.1 Base Score	7.7
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Eran Jacob from OTORIO for coordinated disclosure

ADDITIONAL INFORMATION

Note, that the affected functionality is not available for remote attackers in the default configuration since version V6.0 SP2 of Automation License Manager.

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2023-01-10): Publication Date
V1.1 (2023-03-14): Updated workarounds and mitigations; clarified, that the affected functionality is not available for remote attackers in the default configuration

TERMS OF USE