SSA-388646: Local Privilege Escalation in Automation License Manager

Publication Date: 2020-08-11
Last Update: 2020-08-11
Current Version: V1.0
CVSS v3.1 Base Score: 7.3

SUMMARY

The latest update for Automation License Manager (ALM) fixes a vulnerability that could allow local users to locally escalate privileges and modify files that should be protected against writing.

Siemens has released an update for ALM 6 and recommends that customers update to the latest version. Siemens recommends specific countermeasures for ALM 5 as currently there are no fixes available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Automation License Manager 5: All versions	See recommendations from section Workarounds and Mitigations
Automation License Manager 6: All versions < V6.0.8	Update to V6.0.8 or later version https://support.industry.siemens.com/cs/ww/en/view/114358

WORKAROUNDS AND MITIGATIONS

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

- Disable access to drives which have licenses installed, for non administrator users

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-2020-7583

The application does not properly validate the users' privileges when executing some operations, which could allow a user with low permissions to arbitrary modify files that should be protected against writing.

CVSS v3.1 Base Score	7.3
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-285: Improper Authorization

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Lasse Trolle Borup from Danish Cyber Defence for coordinated disclosure

ADDITIONAL INFORMATION

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 (2020-08-11): Publication Date

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.