SSA-920962: Vulnerabilities in Automation License Manager

Publication Date:	2018-08-07
Last Update:	2018-08-07
Current Version:	V1.0
CVSS v3.0 Base Score:	8.8

SUMMARY

The latest updates for Automation License Manager fix two vulnerabilities. One of them could allow an attacker to execute arbitrary code on the target device, the other one could allow an attacker to abuse the target system for basic network scanning.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Automation License Manager 5: All versions < 5.3.4.4	Update to V5.3.4.4 https://support.industry.siemens.com/cs/ww/en/view/114358
Automation License Manager 6: All versions < 6.0.1 only affected by CVE-2018-11455	Update to V6.0.1 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:

- Restrict network access as far as possible

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 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2018-11455

A directory traversal vulnerability could allow a remote attacker to move arbitrary files, which can result in code execution, compromising confidentiality, integrity and availability of the system. Successful exploitation requires a network connection to the affected device. The attacker does not need privileges or special conditions of the system, but user interaction is required.

At the time of advisory publication no public exploitation of this securtiy vulnerability was known.

CVSS v3.0 Base Score	8.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-11456

An attacker with network access to the device could send specially crafted network packets to determine whether or not a network port on another remote system is accessible or not. This allows the attacker to do basic network scanning using the victims machine.

Successful exploitation requires a network connection to the affected device. The attacker does not need privileges, no user interaction is required. The impact is limited to determining whether or not a port on a target system is accessible by the affected device.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Vladimir Dashchenko from Kaspersky Lab 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 (2018-08-07):   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.