SSA-727467: Vulnerabilities in Building Technologies Products

Publication Date: 2018-03-28
Last Update: 2018-04-03
Current Version: V1.1
CVSS v3.0 Base Score: 9.8

SUMMARY

The License Management System (LMS), which is used by multiple Siemens' building automation products, includes a vulnerable version of Gemalto Sentinel LDK RTE. Gemalto Sentinel LDK RTE is affected by multiple vulnerabilities that could allow remote code execution.

Siemens recommends to update the License Management System used by these products to the newest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
License Management System (LMS): All versions < V2.1 SP3 (2.1.670)	Install LMS V2.1 SP4 (2.1.681) or newer To update to 2.1.681 follow the instructions at https://support.industry.siemens.com/cs/document/109479834 or contact your local Siemens representative or the Siemens customer support.
Annual Shading: V1.0.4, V1.1	Install LMS V2.1 SP4 (2.1.681) or newer To update to 2.1.681 follow the instructions at https://support.industry.siemens.com/cs/document/109479834 or contact your local Siemens representative or the Siemens customer support.
Desigo ABT: MP1.1 Build 845, MP1.15 Build 360, MP1.16 Build 055, MP1.2 Build 850, MP1.2.1 Build 318, and MP2.1 Build 965	Install LMS V2.1 SP4 (2.1.681) or newer To update to 2.1.681 follow the instructions at https://support.industry.siemens.com/cs/document/109479834 or contact your local Siemens representative or the Siemens customer support.
Desigo CC: MP1.1, MP2.0, MP2.1, and MP3.0	Install LMS V2.1 SP4 (2.1.681) or newer. Customers with MP2.1 or older need to upgrade ALM Manager before applying the update to LMS. To update to 2.1.681 follow the instructions at https://support.industry.siemens.com/cs/document/109479834 or contact your local Siemens representative or the Siemens customer support.
Desigo Configuration Manager (DCM): V6.10.140	Install LMS V2.1 SP4 (2.1.681) or newer To update to 2.1.681 follow the instructions at https://support.industry.siemens.com/cs/document/109479834 or contact your local Siemens representative or the Siemens customer support.

Desigo XWP: V5.00.204, V5.00.260, V5.10.142, V5.10.212, V6.00.184, V6.00.342, and V6.10.172	Install LMS V2.1 SP4 (2.1.681) or newer To update to 2.1.681 follow the instructions at https://support.industry.siemens.com/cs/document/109479834 or contact your local Siemens representative or the Siemens customer support.
SiteIQ Analytics: V1.1, V1.2, and V1.3	Install LMS V2.1 SP4 (2.1.681) or newer To update to 2.1.681 follow the instructions at https://support.industry.siemens.com/cs/document/109479834 or contact your local Siemens representative or the Siemens customer support.
Siveillance Identity: V1.1	Install LMS V2.1 SP4 (2.1.681) or newer To update to 2.1.681 follow the instructions at https://support.industry.siemens.com/cs/document/109479834 or contact your local Siemens representative or the Siemens customer support.

WORKAROUNDS AND MITIGATIONS

Siemens has not identified any specific mitigations or workarounds.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure Siemens strongly recommends to protect network access to affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

License Management System (LMS) is the unified license management system for Siemens' building automation products such as Desigo CC and ABT.

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-2017-11496

Malformed ASN1 streams in V2C and similar input files can be used to generate stack-based buffer overflows. The vulnerability could allow arbitrary code execution.

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2017-11497

Language packs containing malformed filenames could lead to a stack buffer overflow. The vulnerability could allow arbitrary code execution.

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2017-11498

Zipped language packs with invalid HTML files could lead to NULL pointer access. The vulnerability could cause denial of service of the remote process.

CVSS v3.0 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 CVE-2017-12818

A stack overflow flaw in the custom XML-parser could allow remote denial of service.

CVSS v3.0 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 CVE-2017-12819

Remote manipulation of the language pack updater could allow NTLM-relay attacks.

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2017-12820

Arbitrary memory read from controlled memory pointer could allow remote denial of service.

CVSS v3.0 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 CVE-2017-12821

A memory corruption flaw could allow remote code execution.

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2017-12822

The administrative interface can be remotely enabled and disabled without authentication. This could increase the attack surface.

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

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Sergey Temnikov and Vladimir Dashchenko from Kaspersky Lab ICS CERT for reporting the vulnerabilities

ADDITIONAL INFORMATION

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 (2018-03-28): Publication Date
V1.1 (2018-04-03): Added download link for LMU

TERMS OF USE