SSA-566773: Vulnerabilities in Building Technologies Products

Publication Date:	2018-06-12
Last Update:	2018-06-12
Current Version:	V1.0
CVSS v3.0 Base Score:	9.6

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 two vulnerabilities that could allow denial-of-service and a cross-site-scripting vulnerability.

Siemens recommends updating the affected dongle driver.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
License Management System (LMS): V2.1 and earlier	Update dongle driver as described here: https://support.industry.siemens.com/cs/document/109758167
Annual Shading: V1.0.4, V1.1	Update dongle driver as described here: https://support.industry.siemens.com/cs/document/109758167
Desigo ABT: V3.1.0, V3.0.1 and earlier (builds 12.10.318, 12.0.850.0, 11.10.55.0, 11.0.360.0, 10.10.845.0 and 10.0.830.0)	Update dongle driver as described here: https://support.industry.siemens.com/cs/document/109758167
Desigo CC / Cerberus DMS: V1.1, V2.0, V2.1, V3.0	Update dongle driver as described here: https://support.industry.siemens.com/cs/document/109758167
Desigo Configuration Manager (DCM): V6.1 SP2 and earlier, V6.0 SP1 and earlier	Update dongle driver as described here: https://support.industry.siemens.com/cs/document/109758167
Desigo XWP: V6.1 and earlier	Update dongle driver as described here: https://support.industry.siemens.com/cs/document/109758167
SiteIQ Analytics: V1.1, V1.2, V1.3	Update dongle driver as described here: https://support.industry.siemens.com/cs/document/109758167
Siveillance Identity: V1.1	Update dongle driver as described here: https://support.industry.siemens.com/cs/document/109758167

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-2018-6304

A stack overflow in the XML-parser of the Gemalto Sentinel LDK RTE can allow an unauthenticated attacker to perform remote denial-of-service attacks without user interaction.

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-2018-6305

A vulnerability of the Gemalto Sentinel LDK RTE can allow an unauthenticated attacker to perform remote denial-of-service attacks without user interaction.

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-2018-8900

A Cross-Site-Scripting vulnerability of the Gemalto Sentinel LDK RTE can allow an unauthenticated attacker to inject script code in the logs page of the Admin Control Center. The script code is executed when an administrative user visits the affected page. Executing script code controlled by an attacker can lead to confidentiality, integrity and availability impact.

CVSS v3.0 Base Score	9.6
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

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 (2018-06-12): 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.