SSA-127490: Vulnerabilities in SIMATIC WinCC Add-Ons

Publication Date: 2018-01-18
Last Update: 2018-02-22
Current Version: V1.1
CVSS v3.0 Base Score: 9.8

SUMMARY

Multiple SIMATIC WinCC Add-Ons released in 2015 and earlier include a vulnerable version of Gemalto Sentinel LDK RTE. Gemalto Sentinel LDK RTE is affected by a vulnerability that could allow remote code execution. Siemens recommends to update the affected software component Gemalto Sentinel LDK RTE.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC WinCC Add-On Historian CONNECT ALARM: All versions <= V5.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PI CONNECT ALARM: All versions <= V2.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PI CONNECT AUDIT TRAIL: All versions <= V1.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PM-AGENT: All versions <= V5.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PM-ANALYZE: All versions <= V7.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PM-CONTROL: All versions <= V10.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PM-MAINT: All versions <= V9.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PM-OPEN EXPORT: All versions <= V7.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce

SIMATIC WinCC Add-On PM-OPEN HOST-S: All versions <= V7.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PM-OPEN IMPORT: All versions <= V6.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PM-OPEN PI: All versions <= V7.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PM-OPEN PV02: All versions <= V1.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PM-OPEN TCP/IP: All versions <= V8.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On PM-QUALITY: All versions <= V9.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On SICEMENT IT MIS: All versions <= V7.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce
SIMATIC WinCC Add-On SIPAPER IT MIS: All versions <= V7.x	Update License Manager software https://supportportal.gemalto.com/csm/?id=kb_article&sys_id=a459d328dba207c8fe0aff3dbf9619ce

WORKAROUNDS AND MITIGATIONS

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

- It is advised to configure the environment according to our operational guidelines (see https://www.siemens.com/cert/operational-guidelines-industrial-security) in order to run the devices in a protected IT environment.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to run the devices in a protected IT environment, Siemens particularly 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

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system. WinCC Add-Ons are developed by partners both inside and outside of Siemens to implement applications that are precisely tailored to the requirements of the industrial plant.

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 (2018-01-18):	Publication Date
V1.1 (2018-02-22):	Added missing CVE references

TERMS OF USE