SSA-844562: Multiple Vulnerabilities in Licensing Software for WinCC OA

Publication Date: 2019-02-25
Last Update: 2019-04-09
Current Version: V1.1
CVSS v3.0 Base Score: 10.0

SUMMARY

Multiple vulnerabilities have been identified in the WibuKey Digital Rights Management (DRM) solution, which affect WinCC OA. Siemens recommends users to apply the updates to WibuKey Digital Rights Management (DRM) provided by WIBU SYSTEMS AG.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC WinCC OA 3.14: All versions < P025	Update to V3.14-P025 or apply WibuKey Digital Rights Management (DRM) version 6.50 or higher from WIBU SYSTEMS AG https://www.winccoa.com/downloads/category/patches-315-16.html
SIMATIC WinCC OA 3.15: All versions < P018	Update to V3.15-P018 or apply WibuKey Digital Rights Management (DRM) version 6.50 or higher from WIBU SYSTEMS AG https://www.winccoa.com/downloads/category/patches-315-17.html
SIMATIC WinCC OA 3.16: All versions < P007	Update to V3.16-P007 or apply WibuKey Digital Rights Management (DRM) version 6.50 or higher from WIBU SYSTEMS AG https://www.winccoa.com/downloads/category/patches-316-1.html

WORKAROUNDS AND MITIGATIONS

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

- CVE-2018-3991 can be mitigated by blocking port 22347/tcp e.g. on an external firewall.

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), 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

 © Siemens AG 2019

PRODUCT DESCRIPTION

The client-server HMI (human machine interface) system SIMATIC WinCC Open Architecture (OA) is part of the SIMATIC HMI family. It is designed for use in applications requiring a high degree of customer-specific adaptability, large or complex applications and projects that impose specific system requirements or functions.

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-2018-3989

A specially crafted IRP (I/O request packet) can cause the driver to return uninitialized memory, resulting in kernel memory disclosure.

CVSS v3.0 Base Score	4.3
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C

Vulnerability CVE-2018-3990

A specially crafted IRP (I/O request packet) can cause a buffer overflow, resulting in kernel memory corruption and, potentially, privilege escalation.

CVSS v3.0 Base Score	9.3
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-3991

A specially crafted TCP packet sent to port 22347/tcp can cause a heap overflow, potentially leading to remote code execution.

CVSS v3.0 Base Score	10.0
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/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 (2019-02-25): Publication Date
V1.1 (2019-04-09): Added solutions

 © Siemens AG 2019

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.