SSA-346256: Vulnerability in SIMATIC WinCC OA V3.14 and prior

Publication Date: 2018-09-11
Last Update: 2018-09-11
Current Version: V1.0
CVSS v3.0 Base Score: 9.1

SUMMARY

The latest update for SIMATIC WinCC OA V3.14 fixes a vulnerability that could allow an unauthenticated remote user to escalate its privileges in the context of SIMATIC WinCC OA V3.14.

This vulnerability affects SIMATIC WinCC OA V3.14 and prior. SIMATIC WinCC OA V3.15 and V3.16 are not affected by this vulnerability.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC WinCC OA V3.14 and prior: All versions < V3.14-P021	Update to V3.14-P021 and follow the steps at https://portal.etm.at/patchdownload.php?fp=version_3.14/win64vc12/ReadmeP021.txt for adding of modifying WinCC OA users in AD environments. https://portal.etm.at/index.php?option=com_content&view=category&id=67&layout=blog&Itemid=80

WORKAROUNDS AND MITIGATIONS

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

- The steps described at https://portal.etm.at/patchdownload.php?fp=version_3.14/win64vc12/ReadmeP021.txt allow manual remediation of the vulnerability fixed by WinCC OA V3.14-P021.
- Follow the SIMATIC WinCC OA Security Guideline (available at https://portal.etm.at/index.php?option=com_phocadownload&view=category&id=52:security&Itemid=81) for maintaining a secured SIMATIC WinCC OA environment.
- Apply Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security

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 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-2018-13799

Improper access control to a data point of the affected product could allow an unauthenticated remote user to escalate its privileges in the context of SIMATIC WinCC OA V3.14.

This vulnerability could be exploited by an attacker with network access to port 5678/TCP of the SIMATIC WinCC OA V3.14 server. Successful exploitation requires no user privileges and no user interaction. This vulnerability could allow an attacker to compromise integrity and availability of the SIMATIC WinCC OA system.

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

CVSS v3.0 Base Score	9.1
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/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 (2018-09-11): 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.

