SSA-822928: Access Control Vulnerability in SIMATIC WinCC OA UI Mobile App for Android and iOS

Publication Date: 2018-03-20
Last Update: 2018-03-20
Current Version: V1.0
CVSS v3.0 Base Score: 5.1

SUMMARY

The latest update for the Android app and iOS app SIMATIC WinCC OA UI fix a security vulnerability which could allow read and write access from one HMI project cache folder to other HMI project cache folders within the app's sandbox on the same mobile device. This includes HMI project cache folders of other configured WinCC OA servers. Precondition for this scenario is that an attacker tricks an app user to connect to an attacker-controlled WinCC OA server.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC WinCC OA UI for Android: All versions < V3.15.10	Update to V3.15.10 https://play.google.com/store/apps/details?id=com.siemens.winccoaui
SIMATIC WinCC OA UI for iOS: All versions < V3.15.10	Update to V3.15.10 https://itunes.apple.com/us/app/simatic-wincc-oa-ui/id1073943068

WORKAROUNDS AND MITIGATIONS

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

- Only connect to trusted WinCC OA Server
- 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.

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

The SIMATIC WinCC OA UI app allows remote access to a SIMATIC WinCC OA facility with the mobile device. The app offers the same functionality as a remote user interface of WinCC OA.

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-2018-4844

Insufficient limitation of CONTROL script capabilities could allow read and write access from one HMI project cache folder to other HMI project cache folders within the app's sandbox on the same mobile device. This includes HMI project cache folders of other configured WinCC OA servers.

The security vulnerability could be exploited by an attacker who tricks an app user to connect to an attacker-controlled WinCC OA server. Successful exploitation requires user interaction and read/write access to the app's folder on a mobile device. The vulnerability could allow reading data from and writing data to the app's folder.

At the time of advisory publication no public exploitation of this security vulnerability was known. Siemens confirms the security vulnerability and provides mitigations to resolve the security issue.

CVSS v3.0 Base Score	5.1
CVSS Vector	CVSS:3.0/AV:A/AC:H/PR:L/UI:R/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Alexander Bolshev from IOActive for coordinated disclosure
- Ivan Yushkevich from Embedi for coordinated disclosure

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 (2018-03-20): 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.