SSA-597741: Vulnerability in iOS App SIMATIC WinCC OA Operator

Publication Date: 2018-04-18
Last Update: 2018-10-09
Current Version: V1.1
CVSS v3.0 Base Score: 4.0

SUMMARY

The SIMATIC WinCC OA Operator iOS app is affected by a security vulnerability which could allow an attacker to read unencrypted data from the application's directory. Precondition for this scenario is that an attacker has physical access to the mobile device.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC WinCC OA Operator iOS App: All versions < V1.4	Update to V1.4 https://itunes.apple.com/app/simatic-wincc-oa-operator/id681238489

WORKAROUNDS AND MITIGATIONS

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

- Toggle off the button to save password while logging in and logout after every work session.
- 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 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 SIMATIC WinCC OA Operator iOS app allows remote access to a SIMATIC WinCC OA facility with the mobile device. The app offers a limited amount of functionality which is programmed into the native app.

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-2018-4847

Insufficient protection of sensitive information (e.g. session key for accessing server) in Siemens WinCC OA Operator iOS app could allow an attacker with physical access to the mobile device to read unencrypted data from the app's directory.

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

CVSS v3.0 Base Score	4.0
CVSS Vector	CVSS:3.0/AV:P/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:T/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 security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2018-04-18):	Publication Date
V1.1 (2018-10-09):	Added update for WinCC OA Operatopr App

TERMS OF USE