SSA-589378: Vulnerabilities in Android App SIMATIC Sm@rtClient

Publication Date 2017-07-13
Last Update 2017-07-13
Current Version V1.0
CVSS v3.0 Base Score 7.4

SUMMARY

The latest update for the SIMATIC Sm@rtClient Android app fixes two vulnerabilities. One of the vulnerabilities could under certain conditions allow an attacker in a privileged network position to read and modify data within a TLS session.

AFFECTED PRODUCTS

- SIMATIC WinCC Sm@rtClient for Android: All versions < V1.0.2.2
- SIMATIC WinCC Sm@rtClient Lite for Android (affected by vulnerability 2): All versions < V1.0.2.2

DESCRIPTION

The Android app SIMATIC WinCC Sm@rtClient, in combination with the SIMATIC WinCC Sm@rtServer, allows remote operation and monitoring of SIMATIC HMI systems.

Detailed information about the vulnerabilities is provided below.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (http://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 assessed by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2017-6870)

The existing TLS protocol implementation could allow an attacker to read and modify data within a TLS session while performing a Man-in-the-Middle (MitM) attack. This vulnerability affects only SIMATIC WinCC Sm@rtClient for Android.

CVSS Base Score 7.4
CVSS Vector CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C

Vulnerability 2 (CVE-2017-6871)

An attacker with physical access to an unlocked mobile device, that has the affected app running, could bypass the app’s authentication mechanism under certain conditions.

CVSS Base Score 4.6
CVSS Vector CVSS:3.0/AV:P/AC:H/PR:L/UI:N/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C

Mitigating Factors

For vulnerability 1, an attacker requires a network position allowing him to capture and manipulate network packets between the mobile device and the remote server.

For vulnerability 2, an attacker must gain physical access to an unlocked mobile device.

SOLUTION

Siemens has released SIMATIC WinCC Sm@rtClient V1.0.2.2 for Android [1, 2, 3, 4, 5] which fixes these vulnerabilities and recommends updating as soon as possible. Updates will be installed automatically if the mobile device is configured accordingly.

It is advised to configure the environment according to operational guidelines [6].

ACKNOWLEDGEMENTS

Siemens thanks the following for their support and efforts:

- Karsten Sohr and Timo Glander from the TZI at the University of Bremen for coordinated disclosure of the vulnerabilities.

ADDITIONAL RESOURCES

[1] The new version of Sm@rtClient can be obtained via Google's Play Store: https://play.google.com/store/apps/details?id=com.siemens.smartclient

[2] The new version of Sm@rtClient for US customers can be obtained via Google's Play Store: https://play.google.com/store/apps/details?id=com.siemens.smartclient_us

[3] The new version of Sm@rtClient can be obtained via Chinese 360 Store: http://zhushou.360.cn/detail/index/soft_id/3598669

[4] The new version of Sm@rtClient Lite can be obtained via Google's Play Store: https://play.google.com/store/apps/details?id=com.siemens.smartclient_lite

[5] The new version of Sm@rtClient Lite for US customers can be obtained via Google's Play Store: https://play.google.com/store/apps/details?id=com.siemens.smartclient_us_lite

[6] An overview of the operational guidelines for Industrial Security (with the cell protection concept): https://www.siemens.com/cert/operational-guidelines-industrial-security

[7] Information about Industrial Security by Siemens: https://www.siemens.com/industrialsecurity

[8] 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 (2017-07-13): Publication Date

DISCLAIMER