SSA-185226: Vulnerabilities in App SPCanywhere

Publication Date 2015-03-05
Last Update 2015-03-05
Current Version V1.0
CVSS Overall Score 5.3

Summary:

The new App SPC Connect (for iOS and Android) replaces the App SPCanywhere (for iOS and Android) to fix several vulnerabilities. The most severe of these vulnerabilities could allow attackers to capture and modify data in sessions protected with SSL/TLS under certain conditions. To exploit the vulnerability an attacker requires a privileged network position (e.g. Man-in-the-Middle).

All vulnerabilities of SPCanywhere are discussed below.

AFFECTED PRODUCTS

- Android Application SPCanywhere: All versions
- iOS Application SPCanywhere: All versions

DESCRIPTION

SPCanywhere and SPC Connect are mobile applications which allow you to access your Siemens SPC intrusion alarm systems remotely via your mobile phone. It allows you to view and control several sites and you can enable or disable your SPC intrusion alarm system, open doors, control outputs and check the status of your installation.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSSv2 scoring system (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 defined by the customer to accomplish final scoring.

Vulnerability 1 (CVE-2015-1595)

The affected App performs unencrypted system ID to IP address lookups. This could allow attackers to obtain the IP address of an intrusion alarm system and to redirect users if the attacker has a privileged network position. This vulnerability affects the Android and iOS version of SPCanywhere.

CVSS Base Score 4.3
CVSS Temporal Score 3.4
CVSS Overall Score 3.4 (AV:N/AC:M/Au:N/C:P/I:N/A:N/E:POC/RL:OF/RC:C)

Vulnerability 2 (CVE-2015-1596)

Improper SSL certificate validation could allow an attacker to capture or modify data in sessions protected with SSL/TLS if the attacker has a privileged network position. This vulnerability affects the Android and iOS version of SPCanywhere.

CVSS Base Score 5.8
CVSS Temporal Score 4.5
CVSS Overall Score 4.5 (AV:N/AC:M/Au:N/C:P/I:P/A:N/E:POC/RL:OF/RC:C)

Vulnerability 3 (CVE-2015-1597)

Unencrypted code loading could allow attackers to inject code and to perform actions on the mobile device based on the applications privileges. An attacker requires a privileged network position to exploit this vulnerability. This vulnerability affects the Android version of SPCanywhere.

CVSS Base Score	6.8
CVSS Temporal Score	5.3
CVSS Overall Score	5.3 (AV:N/AC:M/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C)

Vulnerability 4 (CVE-2015-1598)

The existing storage mechanism for the application specific password could allow attackers with physical access to the mobile device to extract the password. This vulnerability affects the Android version of SPCanywhere.

CVSS Base Score	4.6
CVSS Temporal Score	3.6
CVSS Overall Score	3.6 (AV:L/AC:L/Au:N/C:P/I:P/A:P/E:POC/RL:OF/RC:C)

Vulnerability 5 (CVE-2015-1599)

The existing file system architecture could allow attackers to bypass the access control of SPCanywhere if an attacker has physical access. This vulnerability affects the iOS version of SPCanywhere.

CVSS Base Score	2.1
CVSS Temporal Score	1.6
CVSS Overall Score	1.6 (AV:L/AC:L/Au:N/C:N/I:P/A:N/E:POC/RL:OF/RC:C)

Mitigating factors:

Attackers can only take advantage of the above mentioned vulnerabilities if the following prerequisites are met:

- For vulnerability 1-3: Get a privileged network position to be able to control network traffic of the SPCAnywhere App.
- For vulnerability 4 and 5: Get physical access.

For general SPC users, the Engineer is required to enable the portal interface for the SPC system to be accessible from spcsecure.com used by the SPCanywhere App.

SOLUTION

Siemens has released a new solution SPCconnect which includes a new portal [4], the new firmware update for controller devices [3] and a new mobile application SPCconnect [1, 2] for Android and iOS. The new solution fixes all vulnerabilities and a migration to the new solution is strongly recommended to all users.

SPCanywhere will continue to be available in the App stores for a smooth transition. In the next months the App will be removed from the App Store and Play Store.

ACKNOWLEDGEMENT

Siemens thanks the following for their support and efforts:

- Karsten Sohr, Bernhard Berger, and Kai Hillmann from the TZI-Bremen for coordinated disclosure of vulnerabilities 1-3.
- Stefan Schuhmann for coordinated disclosure of vulnerability 4.
- Kim Schlyter, Seyton Bradford and Richard Warren from FortConsult (NCC Group) for coordinated disclosure of vulnerabilities 4 and 5.

ADDITIONAL RESOURCES

[1] The new App SPC Connect for Android can be obtained via Google's Play Store: https://play.google.com/store/apps/details?id=com.siemens.spcconnect

[2] The new version App SPC Connect for iOS can be obtained via Apple's App Store: https://itunes.apple.com/app/id948318844

[3] Registered users can obtain the new controller firmware version from: https://is.spiap.com/products/intrusion/spc/centrales.html

[4] Further information on the new solution SPC Connect can be found here: http://www.spcconnect.com

[5] For further inquiries on vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT: http://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2015-03-05): Publication Date

DISCLAIMER