Security Notification – IGSS Mobile

8-Feb-2018

Overview

Schneider Electric has become aware of vulnerabilities in the IGSS Mobile (for Android and iOS) product.

Vulnerability Overview

The vulnerabilities identified are:

- Lack of certificate pinning
- Cleartext storage of password and other sensitive data

Product(s) Affected

The product(s) affected:

- IGSS Mobile for Android, version 3.01 and all versions prior
- IGSS Mobile for iOS, version 3.01 and all versions prior

Vulnerability Details

IGSS Mobile app lacks certificate pinning during the TLS/SSL connection establishing process. This issue could allow an attacker to execute a man-in-the-middle attack.

Overall CVSS Score: **6.4 (Medium)**
CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N
CVE ID: CVE-2017-9968 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9968

IGSS Mobile app passwords are stored in clear-text in the configuration file.

Overall CVSS Score: 6.0 (Medium)
CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N
CVE ID: CVE-2017-9969 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9968

Mitigation

An update for Android with the fix for these vulnerabilities is available for download on Google Play:
https://play.google.com/store/apps/details?id=dk.schneiderelectric.igssmobile

An update for iOS with the fix for these vulnerabilities is available on Apple Store:
https://itunes.apple.com/dk/app/igss-mobile/id871698051

Acknowledgements

Schneider Electric would like to thank Alexander Bolshev (IOActive) and Ivan Yushkevich (Embedi) for all their efforts related to identification of this vulnerability.

For More Information

This document is intended to help provide an overview of the identified situation and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric
Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 *8 February 2018*	Original Release

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2018.02.08 17:04:03 -05'00'