Security Notification – EcoStruxure Power Monitoring Expert, Energy Expert (formerly Power Manager), EcoStruxure Power SCADA Operations (formerly PowerSCADA Expert)

15 February 2018

Overview

Schneider Electric® has become aware of a vulnerability in the Flexera FlexNet Publisher component used in the Schneider Electric Floating License Manager (FLM) software. The FLM is used in EcoStruxure Power Monitoring Expert and Energy Expert (formerly Power Manager). It can also be found in EcoStruxure Power SCADA Operations (formerly PowerSCADA Expert) but only with Advanced Reports and Dashboards Module

Vulnerability Overview

Flexera Software reported a vulnerability of its Flexera FlexNet Publisher, **CVE-2016-10395**. This 3rd party component is used within the Schneider Electric Floating License Manager. This vulnerability may allow an unintended user to execute arbitrary code with system privileges.

Product(s) Affected

The product(s) affected:

- EcoStruxure Power Monitoring Expert 8.2 (Standard, DC, HC Editions)
- StruxureWare Power Monitoring Expert 8.1 (Standard, DC, HC Editions)
- StruxureWare Power Monitoring Expert 8.0 (Standard, DC, HC, Buildings Editions)
- StruxureWare Power Monitoring Expert 7.2.x
- Energy Expert 1.x (formerly Power Manager)
- EcoStruxure Power SCADA Operations 8.x (formerly PowerSCADA Expert) (Only with Advanced Reports and Dashboards Module

Vulnerability Details

The vulnerability in the FlexNet Publisher Licensing Service, as documented in CVE-2016-10395, can be exploited to cause an out-of-bounds memory read access and subsequently execute arbitrary code with SYSTEM privileges.

Mitigation

StruxureWare Power Monitoring Expert 7.2.x. Customers

Users on a product release prior to 7.2.2.

- Upgrade to version 7.2.2 and apply the floating licensing manager (FLM) patch

Users on the 7.2.2 version

- Apply the floating licensing manager (FLM) patch

The patch is available here: https://schneider-electric.box.com/s/n2fh1ym594pqvl87kf0zjsigamuryrje

EcoStruxure Power Monitoring Expert 8.x Customers

Users on product releases PME 8.0 or PME 8.1

- Upgrade to PME 8.2 and apply Cumulative Update (CU) 2

Users on product releases PME 8.2

- Apply Cumulative Update (CU) 2.

*NOTE: CU 2 includes all changes in CU1 and the CU2 content.

The patch is available here: https://schneider-electric.box.com/s/kkdikodcksjj1dzngy68ko0j28wct7vb

Energy Expert 1.x (formerly Power Manager) Customers

Users on product releases Energy Expert 1.x (formerly Power Manager)

- Upgrade to Power Manager 1.3 and apply Cumulative Update (CU) 2

Users on product releases Energy Expert 1.3 (formerly Power Manager)

- Apply Cumulative Update (CU) 2

The patch is available here: https://schneider-electric.box.com/s/kkdikodcksjj1dznqy68ko0j28wct7vb

Power SCADA Operations 8.x (formerly PowerSCADA Expert) with Advance Reports Module Only Customers

Users on product releases Advance Reports 8.0 or 8.1

- Upgrade to Advance Reports 8.2 and apply Cumulative Update (CU) 2

Users on product releases Advance Reports 8.2

- Apply Cumulative Update (CU) 2.

*NOTE: CU 2 includes all changes in CU1 and the CU2 content.

The patch is available here: https://schneider-electric.box.com/s/kkdikodcksjj1dznqy68ko0j28wct7vb

*NOTE: Power SCADA Operations 8.x (formerly PowerSCADA Expert) users should also refer to the Citect patch that resolves the same issues. Please refer to notice here: https://www.citect.schneider-electric.com/safety-and-security-central/36-security-notifications/9134-vulnerabilities-within-schneider-electric-floating-license-manager

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 *15 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: 2018.02.15 11:00:25 -05'00'