Schneider Electric Security Notification

Schneider Electric Floating License Manager (V2.2)

14 May 2019 (10 December 2019)

Overview

Schneider Electric is aware of multiple vulnerabilities in the Flexera FlexNet Publisher, which have been addressed in the Schneider Electric Floating License Manager.

A possible exploitation of one of the following Denial-of-Service vulnerabilities would deny the acquisition of a valid license for the legal use of one of the listed products.

Affected Product(s)

Schneider Electric Floating License Manager V2.3.0.0 and earlier.

The Schneider Electric Floating License Manager is used by the following products:

- EcoStruxure Control Expert (only with floating licenses)
- EcoStruxure Hybrid Distributed Control System (formerly known as Plant Struxure PES)
- EcoStruxure Power Monitoring Expert
- Power SCADA Expert
- SoMachine Motion Floating variant
- EcoStruxure Machine Expert (formerly known as SoMachine)

Vulnerability Details

CVE ID: **CVE-2018-20031**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A Denial of Service vulnerability related to preemptive item deletion in lmadmin and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmadmin or the vendor daemon, causing the heartbeat between lmadmin and the vendor daemon to stop, and the vendor daemon to shut down.

CVE ID: **CVE-2018-20032**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A Denial of Service vulnerability related to message decoding in lmadmin and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmadmin or the vendor daemon, causing the heartbeat between lmadmin and the vendor daemon to stop, and the vendor daemon to shut down.

CVE ID: **CVE-2018-20033**

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A Remote Code Execution vulnerability in lmadmin and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier could allow a remote attacker to corrupt the memory by allocating / deallocating memory, loading lmadmin or the vendor daemon and causing the heartbeat between lmadmin and the vendor daemon to stop. This would force the vendor daemon to shut down. No exploit of this vulnerability has been demonstrated.

CVE ID: **CVE-2018-20034**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A Denial of Service vulnerability related to adding an item to a list in lmadmin and vendor daemon components of FlexNet Publisher version 11.16.1.0 and earlier allows a remote attacker to send a combination of messages to lmadmin or the vendor daemon, causing the heartbeat between lmadmin and the vendor daemon to stop, and the vendor daemon to shut down.

Remediation

A fix for these vulnerabilities is available in Schneider Electric Floating License Manager V2.3.1.0 and newer which is available for download below:

https://www.schneider-electric.com/en/download/document/FLM_V2.3.1.0/

Please download and execute the setup file.

The products below have integrated Floating License Manager V2.3.1.0 or newer.

Product	Remediation
EcoStruxure Machine Expert (formerly known as SoMachine)	https://www.schneider-electric.com/en/product-range-download/2226-ecostruxure-machine-expert/#/software-firmware-tab

EcoStruxure Power Monitoring Expert	Fixed in: • PME 9.0 CU2 - https://schneider-electric.app.box.com/s/ahipmmu5rs1b4h0cq4vm3bu6mevzsxop • PME 8.2 Security Update - https://schneider-electric.app.box.com/s/yb390wl3qto8j7jjoev0iu6guhnku3z6
EcoStruxure Hybrid DCS (formerly known as Plant Struxure PES)	Fixed in EcoStruxure Hybrid DCS 2019: https://app.schneider-electric.com/ecostruxure-hybrid-dcs To learn more about EcoStruxure Hybrid DCS 2019 and how to get it, please contact local Schneider Electric representative
EcoStruxure Control Expert	Fixed in Control Expert version V14.1: https://www.se.com/ww/en/download/document/Ecostruxure_Control Expert_V141/

This notification will be updated as other affected products integrate Schneider Electric Floating License Manager V2.3.1.0 or newer.

Product Information

The Schneider Electric Floating License Manager is a common tool that allows users to manage floating licenses for all Schneider Electric software products on an Enterprise License Server, which can be setup in the customer's local network to host his floating licenses. This tool has its own installation that can be delivered together with the software product when the software product offers floating licenses. This tool includes a wizard that guides the customer through the license activation process.

Important Security Advice
The Schneider Electric Floating License Manager installs the FLEXnet License Server communicating via a network connection with the licensed software products and the vendor daemon. This license server offers also a web portal called FLEXnet License Administrator that can be accessed via the Help menu of the Schneider Electric Floating License Manager.

Following best practices protect this license server against security vulnerabilities:

- Expose the license server and vendor daemon ports only to a trusted network
- Enable the Windows Data Execution Prevention (DEP)

Industry Sector

- Industrial Automation Control
- Power Solutions

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

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

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

Schneider Electric Security Notification

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1.0 *14 May 2019*	Original Release
Version 2.0 *10 Sep 2019*	Product information updated (page 2)
Version 2.1 *08 Oct 2019*	Updated remediations for EcoStruxure Power Monitoring Expert (page 3)
Version 2.2 *10 Dec 2019*	Updated remediations for EcoStruxure Hybrid DCS 2019 and EcoStruxure Control Expert (page 3)

Product Security Office

Digitally signed by Product Security Office
Date: 2019.12.09 18:04:11 -05'00'