Schneider Electric Security Notification

Schneider Electric Floating License Manager (V1.3)

14 July 2020 (13 April 2021)

Overview

Schneider Electric has become aware of multiple vulnerabilities in the Flexera FlexNet Publisher which affected and now 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 products listed below.

April 2021 Update: Added *EcoStruxure OPC UA Server Expert* and *Unity Dif (versions prior to 2.5.0.0)* to the list of affected products.

Affected Products

Schneider Electric Floating License Manager V2.4.0.0 and earlier.

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

- EcoStruxure Control Expert (only those with floating license)
- EcoStruxure Control Expert - Asset Link (only those with floating license)
- EcoStruxure Hybrid Distributed Control System (DCS) (formerly known as PlantStruxure PES)
- EcoStruxure Machine Expert (formerly known as SoMachine) (only those with floating license)
- EcoStruxure Machine Expert – Safety (only those with floating license)
- Facility Expert Online
- EcoStruxure OPC UA Server Expert
- EcoStruxure Power Monitoring Expert
- EcoStruxure Power SCADA Operation (formerly known as PowerSCADA Expert and PowerLogic SCADA)
- SoMachine Motion Floating variant
- Easergy Studio
- eConfigure KNX
- EcoStruxure Power Commission
- EcoStruxure Power Design
- EcoStruxure Energy Expert (formerly Power Manager)
- MasterPact Software
- MasterPact Firmware Component

- PowerSuite
- SmartWidget
- TeSys island and TeSys U
- TeSys island and TeSys U Library
- TeSys T
- Unity Dif (version prior to 2.5.0.0)

Vulnerability Details

CVE ID: **CVE-2019-8960**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A Denial of Service vulnerability related to command handling has been identified in FlexNet Publisher lmadmin.exe version 11.16.2. The message reading function used in lmadmin.exe can, given a certain message, call itself again and then wait for a further message. With a particular flag set in the original message, but no second message received, the function eventually returns an unexpected value which leads to an exception being thrown. The result can be process termination.

CVE ID: **CVE-2019-8961**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A Denial of Service vulnerability related to stack exhaustion has been identified in FlexNet Publisher lmadmin.exe 11.16.2. Because the message reading function calls itself recursively given a certain condition in the received message, an unauthenticated remote attacker can repeatedly send messages of that type to cause a stack exhaustion condition.

Remediation

These vulnerabilities are fixed in Schneider Electric Floating License Manager V2.5.0.0, available for download below:

https://www.seupdate.schneider-electric.com/download/SystemConsistency/SWLic/FLM_latest_version/setup_Schneider_ELectric_Floating_License_Manager_latest_sfx.exe

Please download and execute the setup file.

The following workarounds and mitigations can be applied by customers to reduce the risk:

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

Schneider Electric Security Notification

Product Information

The Schneider Electric Floating License Manager is a common tool used to manage floating licenses for Schneider Electric software products on an Enterprise License Server. It can be set up in the customer's local network to host their floating licenses.

This tool has an installation program that can be delivered 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 also offers a web portal called FLEXnet License Administrator that can be accessed via the Help menu of the Schneider Electric Floating License Manager.

Industry Sector

- Industrial Automation Control
- Power Solutions

Learn more about Schneider Electric's product categories here:
www.schneider-electric.us/en/all-products

How to determine if you are affected

In the Windows Control Panel App, open the section "Programs > Programs and Features". You are affected if you have installed Schneider Electric Floating License Manager V2.4.0.0 or earlier.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices:

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow laptops that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.

- Minimize network exposure for all control system devices and 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). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are 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 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

Revision Control:

Version 1.0 *14 July 2020*	Original Release
Version 1.1 *13 August 2020*	Added affected products (page 1)
Version 1.2 *20 August 2020*	Corrected name of *Energy Expert (formerly Power Manager)* (page 1)
Version 1.3 *13 April 2021*	Added *EcoStruxure OPC UA Server Expert* and *Unity Dif (versions prior to 2.5.0.0)* to the list of affected products. (page 1-2)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.04.11 18:24:00 -04'00'