

Important Security Notification

Security Notification – PlantStruxure PES

17-May-2018

Overview

Schneider Electric® has become aware of multiple vulnerabilities in the Flexera FlexNet Publisher component used in the Schneider Electric Floating License Manager software in PlantStruxure PES.

Schneider Electric takes these vulnerabilities very seriously and we have devoted resources to immediately investigate and address these issues. We believe it is critical to consider the whole picture, including safety, security and reliability. Any patches/solutions/mitigations we release will be carefully tested to ensure that they can be deployed in a manner that is both safe and secure.

Vulnerability Overview

The vulnerabilities identified are:

- CVE-2016-10395
- CVE-2017-5571
- CVE-2016-2177

Product(s) Affected

The product(s) affected:

- PlantStruxure PES V4.3 SP1 and prior versions

Vulnerability Details

FlexNet Publisher Licensing Service can be exploited to cause an out-of-bounds memory read access and subsequently execute arbitrary code with SYSTEM privileges.

Overall CVSS Score: 7.8

(CVSS V3 Vector): AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Important Security Notification

CVE ID: CVE-2016-10395

Open redirect vulnerability in the ladmin component in Flexera FlexNet Publisher 11.14.1 and earlier, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.

Overall CVSS Score: 6.1

(CVSS V3 Vector): AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVE ID: CVE-2017-5571

OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) For More Information

Overall CVSS Score: 9.8

(CVSS V3 Vector): AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

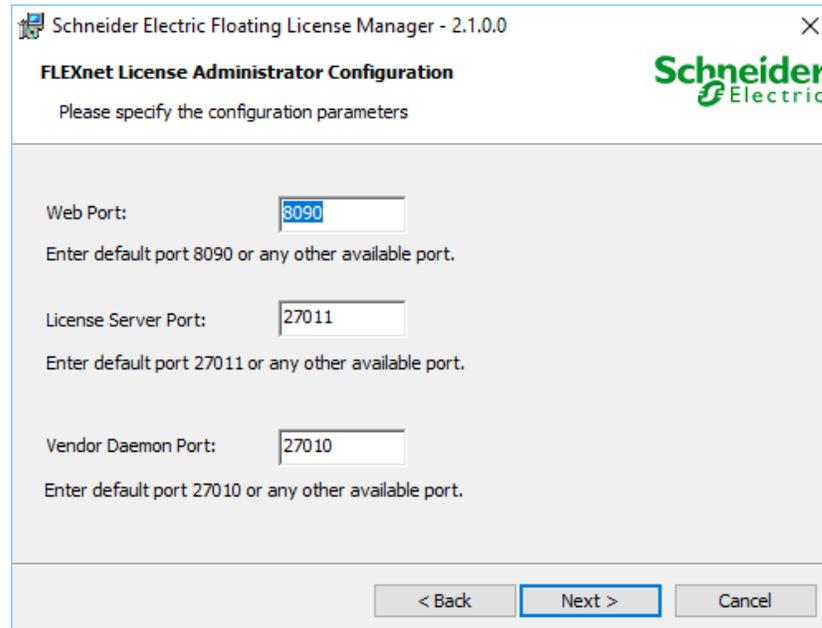
CVE ID: CVE-2016-2177

Mitigation

Schneider Electric has developed a new version of the Floating License Manager which addresses the above vulnerabilities. The Upgrade instructions are detailed below:

- Uninstall your current version of the Floating License Manager
- Install [Floating License Manager v2.1.0.0](#)
- On the "FLEXnet License Administrator" screen, confirm that the "Server Port" is correctly configured for the product that you intend to license.
- **Important Notice:** there is a known issue with the installer of Floating License Manager v2.1.0.0 when installing when a logged-in Windows User name contains a blank. The workaround is to install the Floating License Manager with a user that doesn't include a blank character in their name.

Important Security Notification



The installation of the Floating License Manager will update the port number (27011) in the registry and the same will be read by the License Manager. In case of having the Floating License Server and the PlantStruxure PES system server on another machine, then the user must manually update the License Manager configuration. Please refer to the licensing user guide.

For customers requiring additional support, Schneider Electric's Industrial Cybersecurity Services team are available to help with assessments and deployment support. Please visit us for more information: <https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp>

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>

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND MITIGATION ACTIONS AND IS NOT INTENDED AS A WARRANTY OR GUARANTEE OF ANY KIND, INCLUDING WARRANTIES OF

Important Security Notification

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. WE RESERVE THE RIGHT TO UPDATE OR CHANGE THIS INFORMATION AT ANY TIME AND IN OUR SOLE DISCRETION.

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 <i>17 May 2018</i>	Original Release
--	------------------