Security Notification – PlantStruxure PES License Manager

27-Dec-2016

Overview

Schneider Electric has become aware of a vulnerability in the License Manager component of its PlantStruxure PES platform.

Vulnerability Overview

PlantStruxure PES uses a license manager component provided by Flexera. Flexera reported a vulnerability to its FlexNet Publisher, CVE-2015-8277. This vulnerability could permit a buffer overflow, which could allow remote attackers to execute arbitrary code.

Overall CVSS Score: 9.8

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Product(s) Affected

The products affected include

PlantStruxure PES 4.2 and all previous versions.

Mitigation

This vulnerability is mitigated by upgrading to the new version of the License Manager component in PlantStruxure PES 4.2, available at: http://www.pes.schneider-electric.com/dcs/pes/downloads-updates/product-downloads

.

The upgrade instructions are detailed below:

1. Uninstall your current version of the Floating License Manager

2. Install Floating License Manager v1.9.4.0, available on: http://www.pes.schneider-electric.com/dcs/pes/downloads-updates/product-downloads
3. On the "FLEXnet License Administrator" screen, confirm that the "Server Port" is correctly configured for the product that you intend to license.

Customers unable to upgrade to PlantStruxure PES 4.2 should immediately protect their systems by taking the following steps:

- Utilize the recommended security settings offered by your operating system (OS) vendor that resist buffer/stack overflow attacks.
- Use the Data Execution Prevention (DEP) feature of Windows that helps in this regard.
  o Most OS updates also include hardware and software-based security features that protect against malicious code execution.
- Expose the Flexnet License Administration (lmadmin), including the Schneider Electric daemon, to a trusted network only.

For more information on how to mitigate this vulnerability, please contact the PlantStruxure PES support team via http://www.pes.schneider-electric.com.

For More Information

For further information on other vulnerable Schneider Electric products, please visit the company's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric: Schneider Electric is the global specialist in energy management and automation. With revenues of €27 billion in FY2015, our 160,000 employees serve customers in over 100 countries, helping them to manage their energy and processes in ways that are safe, reliable, efficient and sustainable. From the simplest of switches to complex operational systems, our technology, software and services improve the way our customers manage and automate their operations. Our connected technologies will reshape industries, transform cities and enrich lives. At Schneider Electric, we call this **Life Is On**.

www.schneider-electric.com