Important Security Notification

Security Notification – PlantStruxure PES software environment

27-Dec-2016

Overview

Schneider Electric has become aware of a vulnerability in the PlantStruxure PES software environment.

Vulnerability Overview

A vulnerability associated with the controller simulator within the PlantStruxure PES software environment has been detected. Arbitrary code execution is possible by remotely downloading a patched project file to the simulator.

Product(s) Affected

The product affected:

- PlantStruxure PES software – all versions

Vulnerability Details

Remotely downloading a patched project file to the simulator makes it possible to execute arbitrary, malicious code:

- It is possible to compile a control project mapped on the controller simulator projects with x86 instructions by implanting arbitrary shellcode in the free space of a control project.

- Once the simulator has been started in the PlantStruxure PES environment, the patched project can be downloaded and executed to the simulator.

Overall CVSS Score: 7.5

(CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H)

Mitigation

This vulnerability will be addressed within PlantStruxure PES V4.2, SP3 scheduled for release in Q2 of 2017. Until then, customers should immediately protect their systems by taking the following steps:

1. Protect access to the PlantStruxure PES hosts with a firewall and ensure TCP port 502 is properly filtered.
2. When using the simulator, if possible, disconnect the PC where the controller simulator is running from the network.
3. Close the simulator as soon as simulation testing is over.

For More Information

This document is intended to help provide an overview of the identified vulnerability 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 on vulnerabilities in Schneider Electric's products, please visit Schneider Electric'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

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: 2017.01.03 11:33:55 -05'00'