Important Security Notification

Security Notification – ION Power Meter Cross Site Request Forgery

12-September-2016

Overview

Schneider Electric has become aware of a vulnerability in the ION Power Meter product which could allow unauthorized actions on the device such as configuration parameter changes and saving modified configuration

Product(s) Affected

The product affected:

- ION 73xx, ION 75xx, ION 76xx, ION 8650, ION 8800, PM5xxx

Revenue locking protects meter configuration parameters except Owner, Tag1 and Tag2 string registers.

Vulnerability Details

There is no CSRF Token generated per page and / or per (sensitive) function. Successful exploitation of this vulnerability can allow silent execution of unauthorized actions on the device such as configuration parameter changes, and saving modified configuration.

Successful exploitation of this vulnerability allows silent execution of unauthorized actions on the device, specifically modifying parameter configurations – voltage modes, polarity, voltage units, current units, interval values – by directly sending a POST request, and submitting configuration changes to the meter.

Schneider Electric would like to thank Karn Ganeshen for his discovery efforts during the vulnerability management process.

Mitigation

Configuration parameter changes, as well as saving modified configuration can be prevented for a meter by setting the “Webserver Config Access” register to “Disabled”. This register determines whether or not you can configure your meter through a browser. Valid entries are Enable or Disable. This register is set to Enable by default.

There is also an “Enable Webserver” register. This register enables or disables the webserver entirely. Values for this register are YES and NO. The webserver is enabled by default (the value is set to YES).

Some power meters may be revenue locked which further protects unauthorized meter configuration parameter changes except Owner, Tag1 and Tag2 string registers.

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: 2016.09.15 13:37:34 -04'00'