ION Power Meter Default Password Usage

12-September-2016

Overview

Schneider Electric has become aware of a deployment issue in the ION Power Meter product where it does not enforce a mandatory default password change.

Deployment Overview

The HTTP, Telnet and Front Panel Passwords are configured with default passwords from the factory as defined in documentation. The power meter does not force the end user to change these passwords from the default values.

Product(s) Affected

The products affected:

- ION 7xxx, ION 8x00, ION 8650, PM8000, PM5xxx, iEM3xxx, PM3xxx

Details

Users are strongly encouraged to change their device passwords from default values to prevent unauthorized access. Documentation on security configuration and device password management is available at the following link:

http://www.schneider-electric.us/en/download/document/70012-0260-00/

Schneider Electric would like to thank Karn Ganeshen for his discovery efforts.

Mitigation

All devices that can be accessed using Ethernet must be protected by a properly configured firewall that prevents Telnet access over port 23.

Perform the following actions to help ensure device password-protected security:

- Enable front panel security on your device.
- Ensure the front panel password is not at the default factory value of “0” (zero).
- Make all the device passwords, especially the front panel password, as complex as possible, using the full number of characters available.
- Regularly update the device passwords, especially the front panel password.
- Ensure that your device password information is maintained in a secure location. Password information is required in order to configure your device.

Consult the Instruction Bulletin on configuring security in ION devices located at the following link:
http://www.schneider-electric.us/en/download/document/70012-0260-00/

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 13:36:55 -04'00'