Important Security Notification

Security Notification – PM8ECC Power Meter

27-September-2016

Overview

Schneider Electric has become aware of a vulnerability in the PM8ECC Power Meter product where an unauthenticated attacker can gain full access to the Web interface and FTP service.

Vulnerability Overview

Navigating a web browser to http://<IP or hostname>/status.htm may display a special User: in the top right corner of the browser window. Using this special user as both username and password to login to the meter via HTTP or FTP will allow full administrator access.

Product(s) Affected

The product affected:

- Power Logic PM8ECC, firmware up to 2.651 inclusive

Vulnerability Details

Navigating a web browser to http://<IP or hostname>/status.htm may display a special User: in the top right corner of the browser window. Using this special user as both username and password to login to the meter via HTTP or FTP will allow full administrator access.

The page status.htm is not currently authenticated and when requested independently from webserver's root frameset, may display information in the User: field unintentionally.

Overall CVSS Score: 9.4

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

Schneider Electric would like to thank He Congwen for his discovery and support during the vulnerability management process.

Mitigation

The attack surface can be reduced by turning off the web server. Turning off the web server will not allow the unintentional information to be disclosed. Please contact technical support at Schneider Electric for instructions to turn off the web server. A firmware upgrade to version 2.651 may be required to enable this functionality.

A firmware with the fix for this vulnerability is available for download. Upgrading the PM8ECC firmware version to 2.652 available at the link below will eliminate the vulnerability.

http://www.schneider-electric.com/ww/en/download/document/PM8ECC%2Bv2_DOT_652

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: 2016.10.06 12:50:09 -04'00'