Important Security Notification

Security Notification – Modicon M221

21-Aug-2018

Overview

Schneider Electric has become aware of a vulnerability in the Modicon M221 product.

Vulnerability Overview

The vulnerability identified is Improper Check for Unusual or Exceptional Conditions.

Product(s) Affected

The product(s) affected:

- Modicon M221, all references, all versions prior to firmware V1.6.2.0.

Vulnerability Details

CVE ID: CVE-2018-7789

The vulnerability allows unauthorized users to remotely reboot Modicon M221 using crafted programing protocol frames.

Overall CVSS Score: 4.8

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L

Mitigation

A fix for this vulnerability is implemented in Modicon M221 Firmware V1.6.2.0, delivered within SoMachine Basic V1.6 SP2, which is available for download below or by using Schneider Electric Software Update tool:

https://www.schneider-electric.com/en/download/document/SoMachineBasicV1.6SP2/

As a temporary mitigation, Modicon M221 users should take the following measures:

- Set up a firewall blocking all remote/external access to port 502.
- Within Modicon M221 application, user must disable all unused protocols, especially Programming protocol, as described in section "Configuring Ethernet Network" of SoMachine Basic online help. This will prevent remote programming of the M221 PLCS

Acknowledgements

Schneider Electric would like to thank Yehonatan Kfir of Radiflow for all his efforts related to identification and coordination of this vulnerability.

For More Information

This document is intended to help provide an overview of the identified situation 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 related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND MITIGATION ACTIONS AND IS NOT INTENDED AS A WARRANTY OR GUARANTEE OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. WE RESERVE THE RIGHT TO UPDATE OR CHANGE THIS INFORMATION AT ANY TIME AND IN OUR SOLE DISCRETION.

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 *21 Aug 2018*	Original Release

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: 2018.08.22 06:58:12 -04'00'