Important Security Notification

Security Notification – MiCOM Px4x

15-Mar-2018

Overview

Schneider Electric has become aware of a vulnerability in MiCOM Px4x rejuvenated product.

Vulnerability Overview

The vulnerability identified is on the DNP3oE stack protocol in MICOM Px4x Rejuvenated. It allows denial of service when an attacker sends specially crafted TCP/IP requests to the port 20000 (DNP3oE) of the device.

Product(s) Affected

The product affected includes:

- Within this list of product versions only products with CORTEC digit 9 = “8” (DNP3oE protocol) and last digit = “L” or “M” (Hardware version) are affected
    - MiCOM P540D range:
        - MiCOM P443 version H4
        - MiCOM P445 version H4
        - MiCOM P446 version H4
        - MiCOM All P54x version H4
        - MiCOM P841A version H4
        - MiCOM P841B version H4
    - MiCOM Px4x:
        - MiCOM P14x all versions except B2(B)
        - MiCOM P44x all versions
        - MiCOM P64x all versions
        - MiCOM P746 all versions
        - MiCOM P849 all versions

Security Notification for MiCOM Px4x (P540 range excluded) with legacy Ethernet board (SEVD-2018-074-03) and MiCOM P540D Range with Legacy Ethernet Board (SEVD-2018-02)

Vulnerability Details

Denial of Service

MICOM Px4x Rejuvenated could possibly loss network communication in case of TCP/IP open requests on port 20000 (DNP3oE) if an older TCI/IP session is still open with identical IP address and port number.

Note: The core protection functionalities aren't affected. The protection functions are still fully operational.

Overall CVSS Score: 4.3

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

CVE ID: CVE-2018-7758 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7758

Mitigation

Perform the following mitigation actions to reduce risk:

1. **Secure Network Access (Switch Configuration, Physical Security)**

Secure Network Access is recommended to define strong hardening rules in network devices:

- Disable unused services and port (secure management protocol, physical port, VLAN)
- Use principle of least privilege
- Central account management
- IP filtering
- MAC change notification
- Log management (audit)

2. **Implement a Network Intrusion Detection System**

It is recommended to use advanced firewall in the architecture to detect intrusion on the network. Intrusion Detection System rules must be defined following environments constraints.

Schneider Electric recommends to all customers and users to install mitigation measures and upgrade the firmware of MiCOM Px4x Rejuvenated to the following versions:

Issue resolved in MiCOM P540D range:

- MiCOM P443 versions H6, H7
- MiCOM P445 versions H6, H7
- MiCOM P446 versions H6, H7
- MiCOM P543 to P546 versions H6, H7
- MiCOM P841A versions H6, H7
- MiCOM P841B versions H6, H7

Issue resolved in other MiCOM Px4x:

- MiCOM P14x version B2 (B)
- MiCOM P14x B3
- MiCOM P34x B3/E3
- MiCOM P64x B3
- MiCOM P746 B4/C4
- MiCOM P849 B2

Contact your local support for more information.

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 *15 March 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: 2018.03.15 15:59:35 -04'00'