Security Notification – MiCOM P540D Range with Legacy Ethernet Board

15-Mar-2018

Overview

Schneider Electric has become aware of a vulnerability in the MiCOM P540D range with legacy Ethernet board product.

Vulnerability Overview

The vulnerability identified is on the DNP3oE stack protocol in MiCOM P540D range with legacy Ethernet board product. 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(s) affected:

- Within this list of product versions only products with CORTEC digit 9 = “8” (DNP3oE protocol -enabled) are affected:

  - MiCOM P445 versions: 35, 36, 37, E0, F0*, F1, F2
  - MiCOM P443, P446 versions: 54, 55, 57, B0, D0*, D1, D2
  - MiCOM P543 to P546 versions: 44, 54, 45, 55, 47, 57, A0, B0, C0*, DO*, D1, D2
  - MiCOM P841A versions: 44, 45, 47, A0, C0(*), C1, C2
  - MiCOM P841B versions: 54, 55, 57, B0, D0*), D1, D2

*Excluding minor revision F

Security Notification for MiCOM Px4x (P540 range excluded) with legacy Ethernet board (SEVD-2018-074-03) and MiCOM Px4x rejuvenated product (SEVD-2018-074-04)

Vulnerability Details

Denial of Service

MiCOM P540D range with legacy Ethernet board product could possibly automatically reboot and loss network communication if this vulnerability is exploited. Full denial of service of the MICOM P54x is also possible.

Protection functions are not available during the reboot. At the end of the reboot the product is fully in operation again.

Overall CVSS Score: 6.5

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

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 P540D range with legacy Ethernet board product following these versions:

Issue resolved in:

- P445 versions: F0(F), F3
- P443, P446 versions : D0(F), D3
- P543 to P546 versions: C0(F), D0(F), D3
- P841A versions: C0(F), C3
- P841B versions: D0(F), D3

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

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 15:50:30 -04'00'