Schneider Electric Security Notification

Security Notification – Modicon Quantum

14 May 2019

Overview

Schneider Electric is aware of a vulnerability in its Modicon Quantum product.

Affected Product(s)

Modicon Quantum with firmware versions prior to V2.40.

Vulnerability Details

CVE ID: **CVE-2018-7788**

CVSS v3.0 Base Score 8.8 | (High) | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A CWE-255 Credentials Management vulnerability exists which could cause a Denial Of Service when using a Telnet connection.

Remediation

This vulnerability has been fixed in V2.40. The latest version of Modicon Quantum firmware is V3.5x and is available for download:

https://www.schneider-electric.com/en/download/document/140CPU65260/

Schneider Electric's Modicon Quantum controllers have reached their end of life and are no longer commercially available. They have been replaced by the Modicon M580 ePAC controller, our most current product offer. Customers should strongly consider migrating to the Modicon M580 ePAC.

Product Information

Modicon Quantum: Large PLC for Process applications, high availability & safety solutions. Legacy Range (End of Life communicated December 2018)

Schneider Electric Security Notification

Product Category - Industrial Automation Control

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

Modicon Quantum PLC connected to an Ethernet network using Modbus or Ethernet/IP protocols. Large PLC for Process applications, high availability & safety solutions.

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the "Program" mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2018-7788	Chansim Deng

Schneider Electric Security Notification

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

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

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

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

Schneider Electric Security Notification

Revision Control:

Version 1 *14 May 2019*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2019.05.14 21:58:40 -04'00'