Schneider Electric Security Notification

Security Notification – Modicon Quantum

14 May 2019

Overview

Schneider Electric has become aware of multiple vulnerabilities in its Modicon Quantum product.

Affected Product(s)

Modicon Quantum - all firmware versions

Vulnerability Details

CVE ID: **CVE-2019-6815**

CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE-264: Permissions, Privileges, and Access Control vulnerabilities which could cause a denial of service or unauthorized modifications of the PLC configuration when using Ethernet/IP protocol.

CVE ID: CVE-2019-6816

CVSS v3.0 Base Score 7.4 | (High) | CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:H

CWE-94: Code Injection vulnerability which could cause an unauthorized firmware modification with possible Denial of Service when using Modbus protocol.

Remediation

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 They have been replaced by the Modicon M580 ePAC controller, our most current product offer, which has [insert something here about better imbedded cybersecurity and certifications]. Customers should strongly consider migrating to the Modicon M580 ePAC.

Schneider Electric Security Notification

To mitigate risks associated to Modbus and Ethernet/IP weaknesses on the Modicon Quantum, users should immediately:

- Set up network segmentation and implement a firewall to block all remote/external access to ports 502/TCP, 4418/TCP and 2222/UDP.
- Configure the Access Control List following the recommendations of the user manual "Quantum using EcoStruxure™ Control Expert - 140NOC77101 Ethernet Communication Module, User Manual" Chapter 'Configuring Access Control' available at https://www.se.com/fr/fr/download/document/S1A33985/ or "Quantum using EcoStruxure™ Control Expert - Ethernet Network Modules, User Manual", chapter Access Control' available at https://www.schneider-electric.com/en/download/document/33002479K01000/

Product Information

Modicon Quantum:
Large PLC for Process applications, high availability & safety solutions.
Legacy Range – Phase Out. Progressive end of commercialization starting in Jan 2019.

Market Sector - Industrial Automation Control

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-2019-6815 CVE-2019-6816	Vyacheslav Moskvin and Ivan Kurnakov (Positive Technologies)

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

If you require additional support, Schneider Electric Industrial Cybersecurity Services team are available to help. Please visit: https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND MITIGATION ACTIONS, AND IS PROVIDED ON AN “AS-IS” BASIS 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. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS 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 *14 May 2019*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2019.05.14 22:02:28 -04'00'