Schneider Electric Security Notification

Modicon Controllers (V2.0)

12 November 2019 (14 April 2020)

Overview

Schneider Electric is aware of multiple vulnerabilities impacting its Modicon Controllers offers. The File Transfer Protocol (FTP) is used to transfer configuration files to products to simplify product configuration and to update firmware version. FTP uses hardcoded credentials to automate the file transfer process. The vulnerability exposes the hardcoded credentials. Access to credentials could lead to utilization of these services by unauthorized users, which could lead to unintended controller operation and unintended operation for the devices that connect to the controller FTP server for their configuration files.

Affected Product(s)

All versions of the following product references:

M340 CPUs

BMX P34x

M340 communication modules

BMX NOE 0100
BMX NOE 0110
BMX NOC 0401

Premium CPUs

TSX P57x

Premium communication modules

TSX ETY x103

Quantum CPUs

140 CPU6x

Quantum communication modules

140 NOE 771x1
140 NOC 78x00
140 NOC 77101

Vulnerability Details

CVE ID: **CVE-2019-6852**

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

A CWE-200: Information Exposure vulnerability exists which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.

CVE ID: **CVE-2019-6859**

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

A CWE-798 use of hardcoded credentials vulnerability exists which could cause the disclosure of FTP hardcoded credentials when using the Web server of the controller on an unsecure network.

Remediation

Modicon M340: To mitigate the risks linked to this vulnerability, users should immediately apply the following instructions.

- Set up network segmentation and implement a firewall to block all unauthorized access to port 80/HTTP and port 21/FTP of the controller.
- Deactivate the FTP port and HTTP port when not used, following the recommendations of the user manual “Modicon M340 for Ethernet Communications Modules and Processors User Manual” in chapter “Security”: https://www.schneider-electric.com/en/download/document/31007131K01000/

Modicon Premium and Quantum: Schneider Electric’s Modicon Premium and 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 They have been replaced by the Modicon M580 ePAC controller, our current product offer. Customers should strongly consider migrating to the Modicon M580 ePAC. Please contact your local Schneider Electric technical support for more information.

To mitigate the risks linked to this vulnerability, users should immediately apply the following instructions:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 80/HTTP and port 21/FTP of the controller
- Deactivate the FTP port and HTTP port when not used following the recommendations of the user manual “Premium and Atrium using EcoStruxure™ Control Expert - Ethernet Network Modules, User Manual” in chapters “Security Service Configuration Parameters”: https://www.schneider-electric.com/en/download/document/35006192K01000/

Product Information

Ethernet Programmable Automation Controller for industrial process and infrastructure

Product Category - All Categories

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

How to determine if you are affected

Affected products listed in this security notification connected to an Ethernet network

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Place physical controls so no unauthorized person can access the ICS and safety controllers, peripheral equipment, or the ICS and safety networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow laptops that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and 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). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPNs are 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-2019-6859	VAPT Team from C3i

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

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. 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

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *12-Nov-2019*	Original Release
Version 2 *14-Apr-2020*	Added CVE-2019-6859 (page 2-3)

Product Security Office Digitally signed by Product Security Office
Date: 2020.04.12 23:07:19 -04'00'