Life Is On Schneider Electric

Schneider Electric Security Notification

Modicon Controllers, EcoStruxure™Control Expert and Unity Pro Programming Software (V2.1)

10 December 2019 (15 April 2021)

Overview

Schneider Electric is aware of a vulnerability in the EcoStruxure™ Control Expert and Unity Pro Programming Software.

Affected Products

- EcoStruxure™ Control Expert, all versions prior to 14.1 Hot Fix
- Unity Pro, all versions
- Modicon M340, all versions prior to V3.20
- Modicon M580, all versions prior to V3.10

Vulnerability Details

CVE ID: **CVE-2019-6855**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.0/ AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

A CWE-863: Incorrect Authorization vulnerability exists, which could cause a bypass of the authentication process between EcoStruxure Control Expert and the M340 and M580 controllers.

Remediation

Schneider Electric has made a hotfix available via a free download. After downloading the hotfix, found in the Download Links section below, *all* of the following steps are required to remediate the vulnerability:

STEP 1: Update software and firmware.

- On the engineering workstation, update to EcoStruxure Control Expert V14.1. (Available in the Download Links section.)
    - *Note: Unity Pro software is now named EcoStruxure Control Expert.*
- On the engineering workstation, install EcoStruxure Control Expert V14.1 Hot Fix. (Available in the Download Links section.)

- On the Modicon M340 controller, update to firmware V3.20 or above. (Available in the Download Links section.)
- On the Modicon M580 controller, update to firmware V3.10 or above. (Available in the Download Links section.)

STEP 2: Update projects in EcoStruxure Control Expert.

- Set up an application password in the project properties.
- Change the version of the controller firmware to match the new firmware version of the target controller.

STEP 3: Rebuild and transfer projects in EcoStruxure Control Expert.

- Rebuild all current projects.
- Transfer them to Modicon controllers.

STEP 4: Configure the Access Controls on Modicon controllers.

- Set up network segmentation and implement a firewall to block all unauthorized access to port 502/TCP.

  Modicon M580:

  - Set up secure communication according to “Modicon Controllers Platform Cyber Security Reference Manual” in the chapter “Set up Secured Communication”:

    https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=EIO0000001999.06.pdf&p_Doc_Ref=EIO0000001999

  - Optional -- Additional countermeasure to protect the controller
    Use a BMENOC module and follow the instructions to configure the IPSEC feature described in “Modicon M580 -BMENOC03.1 Ethernet Communications Module, Installation and Configuration Guide” in the chapter “Configuring IP Secure Communications”:
    https://www.schneider-electric.com/en/download/document/HRB62665/#page=1&toolbar=1&scrollbar=1&statusbar=1&view=fit

  Modicon M340:

  - Configure the Access Control List following the recommendations of the user manual “Modicon M340 for Ethernet Communications Modules and Processors User Manual” in the chapter “Messaging Configuration Parameters”:
    https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=31007131_K01_000_16.pdf&p_Doc_Ref=31007131K01000

For assistance enabling the hotfix or to apply these steps, contact our Customer Care Center.

Product Specific Recommendations

- Perform a Self-test.
  - EcoStruxure Control Expert V14.1 will self-test the integrity of its key components when the software is launched. If the results of the test are incorrect, a Windows warning will appear (“Integrity Check – Severe Warning!”) listing the invalid software components. If this happens, the software must be reinstalled. You can perform this test at any time by selecting the Help menu, then choosing About EcoStruxure Control Expert / Perform Self-test.
- Harden the Engineering Workstation.
  - Follow workstation, network, and site-hardening guidelines in the Cybersecurity Best Practices guide available for download here.
- Enable Application Whitelisting.
  - Schneider Electric strongly recommends applying a whitelisting solution to mitigate the risk of this and other vulnerabilities. For assistance with this step, contact our Cybersecurity Services team.

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.
- Put physical controls in place 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.

Download Links

M580 V3.10 Firmware	
BMEP584040	https://www.schneider-electric.com/en/download/document/M580_BMEP584040_SV3.10/
BMEH584040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEH584040_SV3.10/
BMEP586040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEP586040_SV3.10/
BMEH586040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEH586040_SV3.10/
BMEP581020 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP581020_SV3.10/
BMEP582020 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP582020_SV3.10/
BMEP582040 and H	https://www.schneider-electric.com/en/download/document/M580_BMEP582040_SV3.10/
BMEP583020	https://www.schneider-electric.com/en/download/document/M580_BMEP583020_SV3.10/
BMEP583040	https://www.schneider-electric.com/en/download/document/M580_BMEP583040_SV3.10/
BMEP584020	https://www.schneider-electric.com/en/download/document/M580_BMEP584020_SV3.10/
BMEP585040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEP585040_SV3.10/
BMEH582040 and C	https://www.schneider-electric.com/en/download/document/M580_BMEH582040_SV3.10/
BMEP584040S BMEH584040S BMEH586040S BMEP582040S	Contact Schneider Electric Support to receive the firmware version 3.10.

M340 V3.20 firmware	
BMXP3420302 and CL and H	https://www.schneider-electric.com/en/download/document/BMXP3420302_Firmwares/
BMXP342020 and H	https://www.schneider-electric.com/en/download/document/BMXP342020_Firmwares/
BMXP342000	https://www.schneider-electric.com/en/download/document/BMXP342000_Firmwares/
BMXP341000 and H	https://www.schneider-electric.com/en/download/document/BMXP341000_Firmwares/
BMXP3420102 and CL	https://www.schneider-electric.com/en/download/document/BMXP3420102_Firmwares/
BMXP3420302	https://www.schneider-electric.com/en/download/document/BMXP3420302_Firmwares/

EcoStruxure™ Control Expert	
EcoStruxure™ Control Expert V14.1	https://www.se.com/ww/en/product-range-download/548-ecostruxure%E2%84%A2-control-expert/#/software-firmware-tab
EcoStruxure™ Control Expert V14.1 Hot Fix	https://www.se.com/ww/en/download/document/CE_V141_HF_Integrity_Check/

Acknowledgements

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

CVE	Researcher Name(s)
CVE-2019-6855	Rongkuan Ma, Xin Che and Peng Cheng (Zhejiang University) and Enrique Murias Fernández (Tecdesoft Automation)

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.

Schneider Electric Security Notification

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

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 1.0 *10 December 2019*	Original Release
Version 2.0 *14 April 2020*	Updated affected products and remediation section. Added product specific recommendations and download links. Added researcher to acknowledgment sections. (page 1-5)
Version 2.1 *15 April 2021*	Updated CWE for CVE-2019-6855

Product Security Office

Digitally signed by Product Security Office
Date: 2021.04.16 17:14:54 -04'00'