Life Is On Schneider Electric

Schneider Electric Security Notification

Modicon Controllers, EcoStruxure™ Control Expert and Unity Pro Programming Software (V3.0)

20 March 2020 (11 May 2021)

Overview

Researchers from Airbus Cybersecurity have made Schneider Electric aware of a vulnerability in two versions of Schneider Electric's Modicon programmable controllers and its EcoStruxure Control Expert (formerly Unity Pro) programming software.

Since alerting us to the vulnerability, Airbus Cybersecurity and Schneider Electric have collaborated to validate the research and to assess its true impact. Our mutual findings demonstrate that while the discovered vulnerability affects Schneider Electric offers, it equally impacts many other vendors and the global industrial automation market in general, especially when the baseline assumption of the attack technique Airbus Cybersecurity demonstrated is considered. Given certain conditions, and assuming an attacker has access to the network, many devices available from several different industrial control vendors are likewise vulnerable.

Details of the vulnerability and a remediation are included below. However, as a general guideline, Schneider Electric and Airbus Cybersecurity encourage all industrial companies to ensure they have implemented cybersecurity best practices across their operations and supply chains to reduce cyber risks. Where appropriate this includes locating industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; preventing mission-critical systems and devices from being accessed from outside networks; systematically applying security patches and activating antivirus software; and applying whitelisting solutions.

For more detail on Airbus Cybersecurity's research, please visit their blog.

May 2021 Remediation Update: Customers on EcoStruxure™ Control Expert versions prior to V15.0 are recommended to upgrade to remediate CVE-2020-7475.

Affected Products

- EcoStruxure™ Control Expert: *all versions prior to V15.0*
- Unity Pro: *all versions*
- Modicon M340: *all versions prior to V3.20*
- Modicon M580: *all versions prior to V3.10*

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2020-7475**

CVSS v3.0 Base Score 8.2 | High | CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:H/A:H

A *CWE-74: Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection'), reflective DLL*, vulnerability exists, which, if exploited, could allow attackers to transfer malicious code to the controller.

Remediation

After downloading the new version, 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:
  - Recommended remediation: update to EcoStruxure Control Expert V15.0 (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 by:

- Setting up an application password in the project properties
- Changing 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:

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

Modicon M580:

- Setup a secure communication according to the following guideline “Modicon Controllers Platform Cyber Security Reference Manual,” in chapter “Setup secured communications”:

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 IPSEC feature described in the guideline "Modicon M580 - BMENOC03.1 Ethernet Communications Module, Installation, and Configuration Guide" in the chapter "Configuring IPSEC 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 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, please contact our Customer Care Center.

Product Specific Recommendations

- Perform a Self-test:
  - EcoStruxure Control Expert V15 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!***
  - This test can be performed 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, please contact our Cybersecurity Services team.

Schneider Electric Security Notification

General Security Recommendations

We strongly recommend customers and end users always adhere to industry cybersecurity best practices, such as:

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls to prevent unauthorized personnel from accessing your industrial control and safety systems, components, peripheral equipment and networks.
- Put all controllers in locked cabinets and never leave them in the “Program” mode.
- All methods of mobile data exchange with the isolated network, such as CDs, USB drives, etc., should be scanned before being used in the terminals or nodes connected to these networks.
- Laptops that have been connected to any other network besides the network for which it is intended 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 never accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks. However, always recognize that VPNs are also vulnerabilities and should therefore be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

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	Please 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 V15.0	https://www.se.com/ww/en/download/document/EcoStruxure_ControlExpert_V150/

Acknowledgements

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

CVE	Researcher Name
CVE-2020-7475	Flavian Dola, Airbus Cybersecurity

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

Schneider Electric Security Notification

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 1.0 *20 March 2020*	Original Release
Version 2.0 *10 November 2020*	Increased robustness of EcoStruxure Control Expert against the CVE-2020-7475 in software version 15.0 by enabling a new verification mechanism on key components (page 2)
Version 3.0 *11 May 2021*	Remediation Update: Customers on EcoStruxure™ Control Expert versions prior to V15.0 are recommended to upgrade to remediate CVE-2020-7475 (page 2)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.05.08 20:48:40 -04'00'