Schneider Electric Security Notification

Modicon M100/M200/M221 controllers, SoMachine Basic and EcoStruxure Machine Expert - Basic Programming Software

14 April 2020

Overview

Schneider Electric is aware of a vulnerability in the Modicon M100/M200/M221 controllers, SoMachine Basic and EcoStruxure Machine Expert - Basic products.

Affected Product(s)

SoMachine Basic (all versions)
EcoStruxure Machine Expert – Basic (all versions)
Modicon M100 Logic Controller (all versions)
Modicon M200 Logic Controller (all versions)
Modicon M221 Logic Controller (all versions)

Vulnerability Details

CVE ID: **CVE-2020-7489**

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') vulnerability exists in EcoStruxure Machine Expert – Basic or SoMachine Basic programming software. The result of this vulnerability, DLL substitution, could allow the transference of malicious code to the controller.

Remediation

The following workarounds and mitigations can be applied by customers to reduce the risk. All steps are required.

STEP 1: Update software and firmware.

- On the engineering workstation, update to EcoStruxure Machine Expert - Basic V1.0 SP2 or above: https://www.se.com/fr/fr/product-range-download/2226-ecostruxure%E2%84%A2-machine-expert/#/software-firmware-tab
- On Modicon M100/M200/M221 Logic controllers, update to latest firmware version.

STEP 2: Update projects in EcoStruxure Machine Expert – Basic.

- Upgrade the functional level of the application to version 10.2
  Activate the application protection for both read and write in the project properties

STEP 3: Transfer applications.

- Transfer applications to Modicon M100/M200/M221 logic controllers. EcoStruxure Machine Expert – Basic will perform integrity check when transferring the application and will display a warning pop-up to the user if the application has been altered during transfer.

Product Specific Recommendations

- 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.

Product Information

EcoStruxure Machine Expert – Basic and SoMachine Basic are software applications used for developing, configuring, and commissioning the entire machine in a single software environment.

Modicon M100/M200/M221 are Programmable Logic Controllers for machines.

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

Customers using M100/M200/M221 with EcoStruxure Machine Expert – Basic or SoMachine Basic programming software are affected.

Schneider Electric Security Notification

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.

Acknowledgements

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

CVE	Researcher Name(s)
CVE-2020-7489	Seok Min Lim (Trustwave) Johnny Pan (Trustwave)

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

Schneider Electric Security Notification

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 *14 April 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.04.19 21:38:08 -04'00'