Schneider Electric Security Notification

Modicon M218/M241/M251/M258 Logic Controllers, SoMachine/SoMachine Motion, EcoStruxure™ Machine Expert (V1.1)

14 April 2020 (10 November 2020)

Overview

Schneider Electric is aware of multiple vulnerabilities in the Modicon M218, M241, M251 and M258 Logic Controllers, SoMachine & SoMachine Motion, and EcoStruxure Machine Expert products.

The Ecostruxure Machine Expert products are programmable logic controllers and associated programming software.

Failure to apply the remediations provided below may risk denial of service or potential arbitrary code execution.

Nov 2020 Update: Added remediation for M258

Affected Products and Versions

- EcoStruxure Machine Expert (all versions prior to v1.2)
- SoMachine, SoMachine Motion (all versions)
- Modicon M218 Logic Controller (all versions)
- Modicon M241 Logic Controller (all versions prior to v5.0.8.4)
- Modicon M251 Logic Controller (all versions prior to v5.0.8.4)
- Modicon M258 Logic Controller (all versions prior to v5.0.4.11)

Vulnerability Details

CVE ID: **CVE-2020-7487**

CVSS v3.0 Base Score 5.4 | Medium | CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:H

A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers.

CVE ID: **CVE-2020-7488**

CVSS v3.0 Base Score 5.4 | Medium | CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:H

A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers.

Remediation

For Modicon M258 (all versions prior to V5.0.4.11**):**

Modicon M258 offer has been migrated to EcoStruxure Machine Expert v1.2.5. A fix has been implemented for both (CVE-2020-7087 and CVE-2020-7488) vulnerabilities on firmware version V5.0.4.11. We recommend the customer to migrate from the legacy SoMachine application to the new version of EcoStruxure Machine Expert application (https://www.se.com/fr/fr/product-range-download/2226-ecostruxure%E2%84%A2-machine-expert/#/software-firmware-tab) and update the firmware to the latest version through Schneider Electric Software Update (SESU).

For EcoStruxure Machine Expert (all versions prior to v1.2), SoMachine, SoMachine Motion (all versions), Modicon M218 Logic Controller (all versions), Modicon M241 Logic Controller (all versions), Modicon M251 Logic Controller (all versions):

The following workarounds and mitigations should 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 v1.2 or above: https://www.se.com/fr/fr/product-range-download/2226-ecostruxure%E2%84%A2-machine-expert/#/software-firmware-tab
- On Modicon M218/M241/M251 Logic Controllers, update to latest firmware version available through Schneider Electric Software Update (SESU)

Product Specific Reccomendations

Secure the network communications between the engineering workstation and the controllers to ensure trustworthiness.

- 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.

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 inside locked cabinets and never leave them in the “Program” mode.
- Never connect programming software to any network other than the network for the devices 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). Be aware 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 researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher Names
CVE-2020-7487, CVE-2020-7488	Rongkuan Ma, Shunkai Zhu, Peng Cheng (307Lab at Zhejiang University)

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

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 *14 April 2020*	Original Release
Version 1.1 *10 November 2020*	Remediation update for M258 (page 2)

Product Security Office

Digitally signed by Product Security Office
Date: 2020.11.08 20:39:31 -05'00'