Schneider Electric Security Notification

Modicon M258 Logic Controllers and SoMachine/ SoMachine Motion Software

8 December 2020

Overview

Schneider Electric is aware of a vulnerability in its M258 Logic Controllers and SoMachine/ SoMachine Motion software.

The M258 Logic Controllers and SoMachine/SoMachine Motion software are Programmable Logic Controllers and the associated programming software.

Failure to apply the remediations provided below may risk buffer overflow attack, which could result in arbitrary code execution or unavailability of the process or operations.

Affected Products and Versions

Product	Version
Modicon M258 Firmware	All versions prior to V5.0.4.11
SoMachine/SoMachine Motion software	All versions

Vulnerability Details

CVE ID: **CVE-2020-28220**

CVSS v3.0 Base Score 4.3 | Medium | CVSS:3.0/AV:A/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H

A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause a buffer overflow when the length of a file transferred to the webserver is not verified.

Remediation

Version 5.0.4.11 of the Modicon M258 Logic Controller and the new software version of SoMachine/SoMachine Motion (now called EcoStruxure Machine Expert) no longer exhibit this problem.

We recommend customers migrate from the legacy SoMachine/SoMachine Motion software to the new version called EcoStruxure Machine Expert (available here https://www.se.com/ww/en/product-range-download/2226-ecostruxure-machine-expert/ -/software-firmware-tab). Then, update the Modicon M258 Logic Controller firmware to the latest version through Schneider Electric Software Update (SESU). Note: a reboot of the controller is required.

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

- Configure access control lists to restrict web server and FTP access to authorized IP addresses;
- Protect access to Modicon products with network, industrial, and application firewalls.
- Disable web server if not needed.
- Disable FTP server if not needed. This is disabled by default.

To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here:

https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp

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.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and 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 mobile devices 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, understand that VPNs are only as secure as the connected devices.

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

Acknowledgements

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

CVE	Researcher
CVE-2020-28220	Kai Feng

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, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS “NOTIFICATION”) ARE 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 OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, 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. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

Schneider Electric Security Notification

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, 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 with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *8 December 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.12.06 14:25:44 -05'00'