Life Is On Schneider Electric

Schneider Electric Security Notification

Security Notification – SoMachine Basic – Modicon M221

14 February 2019

Overview

Schneider Electric has become aware of multiple vulnerabilities in the Modicon M221 and SoMachine Basic products.

Affected Product(s)

- SoMachine Basic, all versions
- Modicon M221, all references, all versions prior to firmware V1.10.0.0

Vulnerability Details

CVE ID: **CVE-2018-7821**

7.5 | (High) | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

An Environment (CWE-2) vulnerability exists which could cause cycle time impact when flooding the M221 ethernet interface while the Ethernet/IP adapter is activated.

CVE ID: **CVE-2018-7822**

7.7| (High) | AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

An Incorrect Default Permissions (CWE-276) vulnerability exists which could cause unauthorized access to SoMachine Basic resource files when logged on the system hosting SoMachine Basic.

CVE ID: **CVE-2018-7823**

5.3| (Medium) | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

A Environment (CWE-2) vulnerability exists which could cause remote launch of SoMachine Basic when sending crafted ethernet message.

Schneider Electric Security Notification

Remediation

Fixes are available in the Modicon M221 firmware v1.10.0.0 and the EcoStruxure Machine Expert – Basic v 1.0 software (formerly SoMachine Basic) using either of the following options:

- Using Schneider-Electric Software Update tool (SESU)
- https://www.schneider-electric.com/en/download/document/Machine_Expert_Basic

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network 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 not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Schneider Electric Security Notification

Acknowledgements

Schneider Electric would like to recognize the following researcher(s) for all their efforts related to identification and coordination of this vulnerability:

CVE	Researcher Names
CVE-2018-7821	Matthias Niedermaier (Hochschule Augsburg) Jan-Ole Malchow (Freie Universität Berlin) Florian Fischer (Hochschule Augsburg)
CVE-2018-7822 CVE-2018-7823	Reid Wightman (Dragos Inc.)

For More Information

This document is intended to help provide an overview of the identified situation and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

If you require additional support, Schneider Electric Industrial Cybersecurity Services team are available to help. Please visit: https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

Schneider Electric Security Notification

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 *14 February 2019*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2019.02.12 16:25:42 -05'00'