Schneider Electric Security Notification

Modicon M100/M200/M221 Programmable Logic Controller (V3.0)

10 November 2020 (12 January 2021)

Overview

Schneider Electric is aware of multiple vulnerabilities in its Modicon M100, M200, and M221 products.

The Modicon M100/M200/M221 are Nano Programmable Logic Controllers (PLC) made to control basic automation for machines. The M100/M200/M221 are configured using Machine Expert - Basic software.

Failure to apply the mitigations provided below may allow unauthorized users to replay authentication sequences, which could result in an attacker taking control over the PLC.

January 2021 update: Added Modicon M100 and M200 to the list of affected products.

Affected Product and Versions

Modicon M100/M200/M221, all references, all versions

Vulnerability Details

CVE ID: **CVE-2020-7565**

CVSS v3.0 Base Score 7.1 | High | CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

A CWE-326: Inadequate Encryption Strength vulnerability exists that could allow the attacker to break the encryption key when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M100/M200/M221 controllers.

CVE ID: **CVE-2020-7566**

CVSS v3.0 Base Score 7.1 | High | CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

A CWE-334: Small Space of Random Values vulnerability exists that could allow the attacker to break the encryption keys when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M100/M200/M221 controllers.

CVE ID: **CVE-2020-7567**

CVSS v3.0 Base Score 7.1 | High | CVSS:3.0/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

A CWE-311: Missing Encryption of Sensitive Data vulnerability exists that could allow the attacker to find the password hash when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M100/M200/221 controllers and broke the encryption keys.

CVE ID: **CVE-2020-7568**

CVSS v3.0 Base Score 3.1 | Low | CVSS:3.0/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exists that could allow non sensitive information disclosure when the attacker has captured the traffic between EcoStruxure Machine - Basic software and Modicon M100/M200/M221 controllers.

CVE ID: **CVE-2020-28214**

CVSS v3.0 Base Score 3.3 | Low | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

A CWE-760: Use of a One-Way Hash with a Predictable Salt vulnerability exists that could allow an attacker to pre-compute the hash value using dictionary attack technique such as rainbow tables, effectively disabling the protection that an unpredictable salt would provide.

Mitigations

Customers should immediately apply the following mitigations to reduce the risk of exploit:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP.
- Within the Modicon M100/M200/M221 application, the user must:
  - Disable all unused protocols, especially Programming protocol, as described in section "Configuring Ethernet Network" of EcoStruxure Machine Expert - Basic online help for the M100/M200/M221 PLCs. This action will prevent unintended remote programming access.
  - Set a password to protect the project
  - Set a password for read access on the controller
  - Set a different password for write access on the controller

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 researchers for identifying and helping to coordinate a response to this vulnerability:

CVE	Researchers
CVE-2020-7565, CVE-2020-7566, CVE-2020-7567, CVE-2020-7568, CVE-2020-28214	Yehuda Anikster and Rei Henigman of Claroty,
CVE-2020-7566, CVE-2020-7568	Seok Min Lim and Bryon Kaan of Trustwave
CVE-2020-7567, CVE-2020-28214	Seok Min Lim of Trustwave
CVE-2020-7565, CVE-2020-28214	Yangyang Geng, Ke Liu, Houzhi Liu, YaHui Yang, Shunkai Zhu, Peng Cheng, Jie Meng and Mufeng Wang from NESC Lab of Zhejiang University
CVE-2020-7568	Ke Liu, Yangyang Geng and Peng Cheng from NESC Lab of 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, 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

Schneider Electric Security Notification

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.

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 1.0 *10 November 2020*	Original Release
Version 2.0 *8 December 2020*	Added CVE-2020-28214 (page 2)
Version 3.0 *12 January 2021*	Added M100/M200 to the list of impacted products (page 1)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.01.08 17:45:56 -05'00'