Schneider Electric Security Notification

Modicon M221(V1.1)

23 August 2018 (18 September 2020)

Overview

Schneider Electric is aware of multiple vulnerabilities in its Modicon M221 product.

The Modicon M221 is a Nano PLC made to control basic automation for machines. The M221 is configured using SoMachine Basic software.

Failure to apply the remediations provided below may allow unauthorized users to replay authentication sequences, which could result in an attacker having the ability to upload the original program from the PLC.

Affected Product and Version

Modicon M221, all references, all versions prior to firmware V1.6.2.0.

Vulnerability Details

CVE ID: **CVE-2018-7790**

CVSS v3.0 Base Score 9.8 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An Information Management Error vulnerability exists in Schneider Electric's Modicon M221 product (all references, all versions prior to firmware V1.6.2.0). The vulnerability allows unauthorized users to replay authentication sequences. If an attacker exploits this vulnerability and connects to a Modicon M221, the attacker can upload the original program from the PLC.

CVE ID: **CVE-2018-7791**

CVSS v3.0 Base Score 9.8 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A Permissions, Privileges, and Access Control vulnerability exists in Schneider Electric's Modicon M221 product (all references, all versions prior to firmware V1.6.2.0). The vulnerability allows unauthorized users to overwrite the original password with their password. If an attacker exploits this vulnerability and overwrite the password, the attacker can upload the original program from the PLC.

CVE ID: **CVE-2018-7792**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Schneider Electric Security Notification

A Permissions, Privileges, and Access Control vulnerability exists in Schneider Electric's Modicon M221 product (all references, all versions prior to firmware V1.6.2.0). The vulnerability allows unauthorized users to decode the password using rainbow table.

Remediation

A fix for CVE-2018-7790 and CVE-2018-7792 is implemented in Modicon M221 Firmware V1.6.2.0, delivered within SoMachine Basic V1.6 SP2, which is available for download below or by using Schneider Electric Software Update tool:

https://www.schneider-electric.com/en/download/document/SoMachineBasicV1.6SP2/

All the vulnerabilities are fixed on latest version of Modicon M221 Firmware V1.1, delivered within Ecostruxure Machine Expert - Basic V1.1 (current named version of SoMachine Basic), which is available for download below or by using Schneider Electric Software Update tool:

https://www.se.com/ww/en/download/document/Machine_Expert_Basic/

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

- Set up a firewall blocking all unauthorized access to port 502.
- Within Modicon M221 application, 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 M221 PLC. 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.

Acknowledgements

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

CVE	Researcher(s) Name
CVE-2018-7790, CVE-2018-7791, CVE-2018-7792	Irfan Ahmed (University of New Orleans), Hyunguk Yoo (University of New Orleans), Sushma Kalle (University of New Orleans), Nehal Ameen (University of New Orleans),

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 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

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 *23 August 2018*	Original Release
Version 1.1 *18 September 2020*	CVE-2018-7791 fixed on latest version of Modicon M221 controller

Product Security Office

Digitally signed by Product Security Office
Date: 2020.09.18 16:46:26 -04'00'