Security Notification – Modicon M221 / SoMachine Basic – Version B

16-June-2017

Overview

Schneider Electric has become aware of research and a vulnerability identified against the Modicon M221 PLC family of devices that allows an unauthenticated user to transfer a logic controller application into a SoMachine Basic project.

Vulnerability Overview

The Application Protection feature intended to protect against the unauthorized transfer of the application from a logic controller into a SoMachine Basic project, can be compromised by sending a specifically crafted command via Modbus over TCP port 502 to the logic controller, at which point, the controller will return the password. A malicious user could then upload malicious applications and/or lock out legitimate users.

Overall CVSS Score: 10 (Critical)

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L

CVE ID: CVE-2017-7575 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7575

Product(s) Affected

The product(s) affected:

- All Modicon M221 PLCs with firmware version up to v1.5.0.1 and associated SoMachine Basic software (up to v1.5)

Mitigation

A fix to prevent M221 from returning the password to unauthenticated is available within Firmware v1.5.1.0 and associated SoMachineBasic V1.5SP1, released on June the 14th, 2017.

SoMachineBasic V1.5SP1 (including firmware v1.5.1.0) can be downloaded from http://www.schneider-electric.com/en/download/document/SOMBASAP15SP1SOFT/ or by using Schneider Electric Software Update tool.

Acknowledgements

Schneider Electric would like to credit Simon Heming, Maik Brüggemann, Hendrik Schwartke, Ralf Spenneberg of Open Source Security for their identification of this vulnerability.

For More Information

This document is intended to help provide an overview of the identified vulnerability 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 on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

Schneider Electric is the global specialist in energy management and automation. With revenues of ~€25 billion in FY2016, our 160,000+ employees serve customers in over 100 countries, helping them to manage their energy and process in ways that are safe, reliable, efficient and sustainable. From the simplest of switches to complex operational systems, our technology, software and services improve the way our customers manage and automate their operations. Our connected technologies reshape industries, transform cities and enrich lives. At Schneider Electric, we call this **Life Is On**.

www.schneider-electric.com

Revision Control:

Version A *7 April 2017*	Original Release
Version B *16 June 2017*	Page 1 - Updated **Vulnerability Overview** section with CVE ID Page 2 - Updated **Mitigation** section with security update link

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2017.06.16 11:25:36 -04'00'