Schneider
Electric

Security Notification – Modicon M241/M251

16-Mar-2017

Overview

Schneider Electric has become aware of a vulnerability in the Modicon product.

Vulnerability Overview

The vulnerability identified authentication vulnerabilities in PLC embedded web applications (session cookie).

Product(s) Affected

The product(s) affected:

- Schneider Electric Modicon M241
- Schneider Electric Modicon M251

Vulnerability Details

The issue is related to the method that the web application uses to maintain authenticated sessions.

The session numbering is lacking randomization and is shared between several users. This could allow for hacking of currently opened sessions by using a specially crafted cookie.

Overall CVSS Score: 5.4 (medium)

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

Mitigation

Firmware with the fix for this vulnerability is available in SoMachine V4.2 (available through Schneider Electric Software Update tool).

- Schneider Electric Modicon M241 firmware: v4.0.5.11
- Schneider Electric Modicon M251 firmware: v4.0.5.11

The following improvements are implemented in the firmware in order to correct this vulnerability:

- Cookie session string randomization improvement
- Cookie session string no longer shared between users
- Logout button added to Website

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