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 (credentials).

Product(s) Affected

The product(s) affected:

- Schneider Electric Modicon M241
- Schneider Electric Modicon M251

Vulnerability Details

The vulnerability identified that log-in credentials are sent over the network in clear text Base64 encoding. Attackers observing clear text user credentials may then be able to log in to the web application and perform unauthorized data monitoring or potentially stop the controller.

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

To minimize potential exposure, PLC users are advised to consider the recommendations bellow in light of their perceived exposure and risk:

General Security Best Practices

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Ensure physical security of all control system devices and/or systems.
- Perform a hazard and risk analysis that considers all hazards resulting from access to (and operation on) PLC devices, and develop cybersecurity and disaster recovery (business continuity) plans accordingly.
- Verify that the hardware and software infrastructure that the PLCs are integrated into (along with all organizational measures and rules covering access to the infrastructure) consider the results of the hazard and risk analysis, and are implemented according to best practices and standards such as ISA/IEC 62443.
- Verify the effectiveness of the IT security and cybersecurity systems using appropriate, proven methods

Additional Mitigations (Local Area Network)

- Place control system networks and devices behind firewalls (such as the ConneXium Tofino Firewalls), and isolate them from the business network
- Limit traffic on the local network with managed switches (such as ConneXium managed switches)
- Where possible, avoid Wi-Fi capabilities
- When Wi-Fi is essential, use only secure communications (such as WPA2 encryption)
- Do not grant access to unknown computers

Additional Mitigations (Wide Area Network)

- When remote access is essential, use secure methods such as Virtual Private Networks (VPNs), and ensure the remote access solution(s), as well as the remote computer(s) are kept up-to-date with the latest security patches.

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

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: 2017.03.16 11:50:28 -04'00'