Security Notification – M221, M241 RSA Conference Presentation

17-Feb-2017

Overview

Schneider Electric has become aware of a presentation and resulting news articles on the threat of ransomware to exposed or otherwise vulnerable Programmable Logic Controllers (PLCs).

Research was presented by David Formby of the Georgia Institute of Technology at an RSA conference event during a February 13th session, and subsequently reported by news media outlets.

Conscious about user Cyber Security concerns, Schneider Electric places a high priority on the evaluation of security research as it becomes available, and producing documentation to advise PLC users on mitigations that can be taken if they are required.

Proof of Concept Overview

While no product vulnerabilities were identified as part of the research, the use cases presented demonstrate a specific threat scenario where an attacker could utilize limited security protection on existing product to potentially reprogram a Modicon M221 with new passwords, locking legitimate users out of the official programming software.

Product(s) Affected

Schneider Electric Modicon M221

Proof of Concept Details

The devices that were used for this proof of concept version of the LogicLocker PLC worm included a Schneider Modicon M221 and a Schneider Modicon M241. The attack, as described in the research:

- First identified and targeted an internet facing Modicon M241
- Acquired the password via brute force, a weak password, or stolen legitimate credentials

- Used the acquired credentials to load an alternate program, namely the LogicLocker PLC worm (implemented as an application)
- LogicLocker was then used to scan the internal network for vulnerable PLCs to carry out the second stage of the attack.
- The M221's application program is uploaded and held for future use.
- An unprotected Modicon M221 is then reprogrammed with a new application.
- An attacker would then manually encrypt the stolen program on their own machine, using an encryption mechanism of their choice, along with a key generated for the ransomware victim. The program is sold back to the end user to download if the ransom is paid.

Mitigation

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

Configure M221 security settings:

- Minimize attack surface by disabling all unused protocols, especially Programming protocol, as described in section "Configuring Ethernet Network" of SoMachine Basic online help. This will prevent remote programming of the M221 PLC.
- Minimize information disclosure by activating password protection on the application, as described in section "Project Properties" of SoMachine Basic online help.
    - Disable application upload.
- Backup the PLC application to a remote, offline storage location.
- Create an SD Card for application restore in the event that a PLC program is overwritten or lost and remote programming is disabled, as advised above.

Configure Network neighborhood (Modicon M241)

- Minimize attack surface by activating User Management, enforcing passwords and separating roles. The programming protection of the M241 is enforced in the PLC itself and separate passwords can be used for read only, programming etc.
- Minimize attack surface by disabling all unused protocols and configuring the M241 to allow only trusted IP/MAC addresses to connect. Utilize an internal firewall, as described in "Firewall Configuration" section of SoMachine online help.

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 research and actions required to mitigate any potential risk. 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 regarding cybersecurity of 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

References

Connexium Tofino Firewall:
http://www.schneider-electric.fr/fr/download/document/NHA1573401/

Connexium Managed Switch:
http://www.schneider-electric.com/ww/en/download/document/31007122K01000

About Schneider Electric: Schneider Electric is the global specialist in energy management and automation. With revenues of €27 billion in FY2015, our 160,000 employees serve customers in over 100 countries, helping them to manage their energy and processes 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 will 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: 2017.02.22 09:19:09 -05'00'