Security Notification – Modicon

23-May-2017

Overview

Schneider Electric has become aware of a vulnerability. It impacts the Modicon family of PLCs, specifically when replaying run/stop and upload/download requests in the Modbus protocol commands.

Vulnerability Overview

Because the vulnerability concerns the replay of run/stop and upload/download Modbus requests, it could potentially allow a malicious attacker to execute unwanted commands on the target PLC.

Product(s) Affected

Schneider Electric has confirmed that every Modicon PLC could be vulnerable to this type of attack if certain protections are disabled.

The following cannot mitigate this vulnerability with built-in features:

- Modicon Momentum M1E 171CBU98090 (All versions)
- Modicon Momentum M1E 171CBU98091 (All versions)

The following already have mechanisms that protect them from this type of attack, but additional security measures should be taken to improve resiliency:

- Modicon M340 (All versions prior to V2.70)
- Modicon M580 (All versions prior to V2.01)
- Modicon Premium (All versions prior to V3.10)
- Modicon Quantum (All versions prior to V3.12)

The following is impacted if certain protections are disabled:

- Modicon M221 (All versions)

Overall CVSS Score: 7.5 (High)

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

CVE ID: CVE-2017-6028: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6028

Mitigations

Modicon Momentum M1E users must protect access to their M1E controllers by a firewall blocking all remote/external access to port 502.

Modicon M340, Modicon M580, Modicon Premium and Modicon Quantum should take one or more of the following measures:

- Enable protection based on an authentication to connect to PLC. This method relies on a feature named *Application Password*. Once enabled, password-based authentication is required whenever a user connects to change their application program.
- Enable protection relying on an input (M340, Premium, Quantum) or a key switch in the front panel (Quantum) to reject remote connection or run/stop commands.
- Enable the “Access Control List protection”, where users are able to configure the restricted IP addresses that are pre-authorized to control the PLC.

Modicon M221 users should take the following measures:

- Set up a firewall blocking all remote/external 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 SoMachine Basic online help. This will prevent remote programming of the M221 PLC.

Acknowledgement

Schneider Electric would like to thank Eran Goldstein of CRITIFENCE Critical Infrastructure and SCADA/ICS Cyber Threats Research Group for discovery and responsible disclosure support.

For More Information

For further security-related information on Schneider Electric products, please visit the company’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 $26 billion US dollars (25 billion euros) 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: 2017.05.23 14:25:19 -04'00'