Life Is On Schneider Electric

Schneider Electric Security Notification

Modicon Controllers and SCADAPack RTU (V3.0)

23 May 2017 (13 August 2019)

Overview

Schneider Electric is aware of a vulnerability in the Modicon Controller and SCADAPack RTU products.

Affected Product(s)

- Modicon Momentum M1E 171CBU98090 (All versions)
- Modicon Momentum M1E 171CBU98091 (All versions)
- 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)
- Modicon M221 (All versions)
- SCADAPack 32 RTU (All Versions)
- SCADAPack 300 series RTU (314, 330, 334, 350) (All Versions)
- SCADAPack 300 E and 500 E series RTU (312E, 313E, 314E, 330E, 333E, 337E, 350E, 530E, 535E) (All Versions)
- SCADAPack 57x RTU (570, 575) (All Versions)

Vulnerability Details

CVE ID: **CVE-2017-6034**

CVSS v3.0 Base Score 9.8 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

An Authentication Bypass by Capture-Replay issue was discovered in Schneider Electric Modicon Modbus Protocol. Sensitive information is transmitted in cleartext in the Modicon Modbus protocol, which may allow an attacker to replay the following commands: run, stop, upload, and download.

Remediation

The following workarounds and mitigations can be applied by customers to reduce the risk:

- 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 immediately 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 immediately 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.
- SCADAPack RTU users should immediately take the following measures:
    - Set up a firewall blocking all remote/external access to port 502.
    - Within SCADAPack RTUs Configuration software, user must disable all unused protocols, especially programming protocol, as described in:
        - Section “Configuring IP Communication” of SCADAPack 57x Series online help.
        - Section “IP Settings” of SCADAPack 32 and 300 Series.
        - Section “TCP/IP Folder” of SCADAPack 300E and 500E Series.

Product Information

Modicon Controllers: Ethernet Programmable Automation Controller for industrial process and infrastructure

SCADAPack RTU: RTU combining capabilities of remote terminal units with the power of Programmable Logic Controller and designed to run in remote environment.

Product Category - All Categories

Learn more about Schneider Electric’s product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

If you use the Modbus service on one of the affected products versions, your solution is affected.

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2017-6034	- Eran Goldstein of CRITIFENCE Critical Infrastructure and SCADA/ICS Cyber Threats Research Group - Benjamin Green of Lancaster University - Seok Min Lim of Trustwave Research Firm

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative and/or Schneider Electric Industrial

Schneider Electric Security Notification

Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *23 May 2017*	Original Release
Version 2 *09 Jul 2019*	- Updated affected products section to include SCADAPack RTUs (page 1) - Updated remediation section to include information for SCADAPack RTUs (page 2) - Updated researcher acknowledgment section (page 4)
Version 3 *13 Aug 2019*	- Updated researcher acknowledgement section (page 4) - Corrected CVE ID from CVE-2017-6028 to CVE-2017-6034 and corrected vulnerability description (page 1)

Product Security Office

Digitally signed by Product Security Office
Date: 2019.08.13 16:22:41 -04'00'