Life Is On Schneider Electric

Schneider Electric Security Notification

Modicon Controllers (V2.0)

16 March 2017 (13 October 2020)

Overview

Schneider Electric is aware of a vulnerability in its Modicon Controllers products.

The Modicon PLC (Programmable Logic Controllers) and PACs (Programmable Automation Controllers) control and monitor industrial operations in a sustainable, flexible, efficient and protected way.

Failure to apply the remediations and mitigations provided below may risk the disclosure of webserver credentials over the network, which could result in unauthorized operations.

Affected Products and Versions

- Modicon M241 Logic Controller, firmware version prior to 5.0.8.4
- Modicon M251 Logic Controller, firmware version prior to 5.0.8.4
- Modicon Quantum Co-processors ref. 140CPU6*
- Modicon Premium Co-processors ref. TSXP* and TSXH*
- Modicon Quantum Ethernet communication modules ref.140NOE* and 140NOC*
- Modicon Premium Ethernet communication modules ref. TSXETY*
- Modicon M340 CPU ref. BMXP34*
- Modicon M340 Ethernet communication Modules ref. BMXNOC*, BMXNOE*, BMXNOR*
- Modicon Momentum Ethernet MDI

Vulnerability Details

CVE ID: **CVE-2017-6028**

CVSS v3.0 Base Score 8.3 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:L/A:H

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

Remediation

Modicon M241, M251

Version 5.0.8.4 of the Modicon M241/M251 logic controllers include a fix for this vulnerability and is available for download through Schneider Electric Software Update (SESU). A reboot is needed.

Modicon Premium, Quantum, M340 and Momentum

For Modicon PAC impacted products mentioned in the above Affected Product and Version section, Customers are advised:

- that the web service is disabled by default. Because web services are only necessary for specific maintenance, configuration or monitoring activities, it is advised to disable them when the services are not needed. Leaving these services enabled increases your system's vulnerability to cyberattacks.
- to configure access control list to restrict web server access to authorized IP addresses

Please refer to "Modicon Controllers Platform Cyber Security Reference Manual" for detailed instruction on how disable web services and apply other recommendations.

https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=EIO0000001999.07.pdf&p_Doc_Ref=EIO0000001999

For Modicon Momentum Ethernet MDI, please refers to "Momentum for EcoStruxure™ Control Expert 171 CBU 78090, 171 CBU 98090, 171 CBU 98091 Processors User Guide"

https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=HRB44124.07.pdf&p_Doc_Ref=HRB44124

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center (hyperlinked) if you need assistance removing a patch.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.

- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and 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). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are 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	Researchers Name
CVE-2017-6028	David Formby and Raheem Beyah of Georgia Tech and Fortiphyd Logic, Inc Kai Wang of Fortinet's FortiGuard Labs

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

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Schneider Electric Security Notification

DAMAGES. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

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 *16 March 2017*	Original Release
Version 2.0 *13 October 2020*	Updated products affected, vulnerability details, remediation, and acknowledgement sections (page1-3)

Product Security Office

Digitally signed by Product Security Office
Date: 2020.10.10 17:17:46 -04'00'