Schneider Electric Security Notification

Security Notification – Modicon and PacDrive Controllers

14 May 2019

Overview

Schneider Electric is aware of a vulnerability in its line of Modicon process controllers and PacDrive products.

Affected Product(s)

- Modicon M100 - all versions
- Modicon M200 - all versions
- Modicon M221 - all versions
- ATV IMC drive controller - all versions
- Modicon M241 - all versions
- Modicon M251 - all versions
- Modicon M258 - all versions
- Modicon LMC058 - all versions
- Modicon LMC078 - all versions
- PacDrive Eco - all versions
- PacDrive Pro - all versions
- PacDrive Pro2 - all versions

Vulnerability Details

CVE ID: **CVE-2019-6820**

CVSS v3.0 Base Score: 7.1 | (High) | CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

A CWE-306: Missing Authentication for Critical Function vulnerability exists which could cause a modification of device IP configuration (IP address, network mask and gateway IP address) when a specific Ethernet frame is received.

Remediation

Customers should immediately apply the following workarounds and mitigations to reduce risks:

- For Modicon M100, Modicon M200 and Modicon M221:
  - Deactivate the “Auto discovery protocol enable” option in security section of Ethernet configuration page
- For ATV IMC Drive Controller:
  - Deactivate the “Discovery protocol active” option in security section of Ethernet configuration page
- For Modicon M241, Modicon M251, Modicon M258, Modicon LMC058 and Modicon LMC078:
  - Either deactivate the “Discovery protocol active” option in the security section of Ethernet configuration page(s)
  - Or configure the internal firewall in order to block all access to UDP ports 27126 and 27127 (please refer to “Firewall configuration” section of the controller’s online help).
- For PacDrive Eco, Pro and Pro2:
  - Set up a firewall blocking all unauthorized access to UDP ports 27126 and 27127.

Product Information

Affected products are logic controllers for Industrial Machines and automation solutions for motion-centric machines.

Product Category - Industrial Automation Control

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

How to determine if you are affected

Affected products listed in this security notification connected to an Ethernet network.

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-2019-6820	Yehuda A (Claroty)

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 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

Schneider Electric Security Notification

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 *14 May 2019*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2019.05.14 21:47:55 -04'00'