

Schneider Electric Security Notification

Use of Hard-coded Credentials vulnerability on Easergy MiCOM Px40 Series

14 April 2026 (12 May 2026)

Overview

Schneider Electric is aware of a vulnerability in its Easergy MiCOM Px40 Series products.

The [Easergy MiCOM Px40](#) is a protection relay series for Medium Voltage, High Voltage and Extra High Voltage protection.

Failure to apply the mitigations provided below may risk unauthorized exposure of basic device identification through the SNMP protocol.

May 2026 Update: Updated the risk associated with successful exploitation of this vulnerability and revised the remediation table to a mitigation table to emphasize that multiple mitigation options are available.

Affected Products and Versions

Only Easergy MiCOM Px40 models with the Ethernet option are affected. Models with the ethernet option can be identified using the model number as Q, R, S indicated in the 7th digit of the model number.

Product	Version
Easergy MiCOM P14x	All versions prior to B4A
Easergy MiCOM P24x	All versions prior to D3A
Easergy MiCOM P341	All versions prior to E3F
Easergy MiCOM P342, P343, P344, P345	All versions prior to B3F
Easergy MiCOM P442, P444	All versions prior to E3A
Easergy MiCOM P443, P445, P446, P543, P544, P545, P546	All versions prior to H6A
Easergy MiCOM P841	All versions prior to G6A
Easergy MiCOM P643	All versions prior to B3F
Easergy MiCOM P642, P645	All versions prior to B4A
Easergy MiCOM P741, P742, P743	All versions prior to B2A
Easergy MiCOM P746	All versions prior to B4E or C4E
Easergy MiCOM P849	All versions prior to B4A

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2026-4832**

CVSS v3.1 Base Score 5.3 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVSS v4.0 Base Score 6.9 | Medium | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

CWE-798 Use of Hard-coded Credentials vulnerability exists that could cause unauthorized access to sensitive device information when an unauthenticated attacker is able to interrogate the SNMP port.

The severity of vulnerabilities was calculated using the CVSS Base metrics for 4.0 ([CVSS v4.0](#)). CVSS v3.1 will be still evaluated until the adoption of CVSS v4.0 by the industry. The severity was calculated without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Mitigation

Affected Product & Version	Mitigation
Easergy MiCOM P14x <i>All versions prior to B4A</i>	<p>For customers who do not require SNMP Contact Schneider Electric's Customer Care Center to upgrade the Firmware to a version without SNMP functionality.</p> <p>If customers choose not to apply the upgrade provided above, they should immediately apply the following mitigations to reduce the risk of exploit:</p> <ul style="list-style-type: none"> • Use relays only in a protected network environment, • Use firewalls to protect and separate the control system network from other networks, • Use VPN (Virtual Private Networks) tunnels if remote access is required. <p>For customers who require SNMP Please immediately apply the following mitigations to reduce the risk of exploit:</p> <ul style="list-style-type: none"> • Use relays only in a protected network environment, • Use firewalls to protect and separate the control system network from other networks, • Use VPN (Virtual Private Networks) tunnels if remote access is required.
Easergy MiCOM P24x <i>All versions prior to D3A</i>	
Easergy MiCOM P341 <i>All versions prior to E3F</i>	
Easergy MiCOM P342,P343,P344,P345 <i>All versions prior to B3F</i>	
Easergy MiCOM P442, P444 <i>All versions prior to E3A</i>	
Easergy MiCOM P443, P445, P446, P543, P544, P545, P546 <i>All versions prior to H6A</i>	
Easergy MiCOM P841 <i>All versions prior to G6A</i>	
Easergy MiCOM P643 <i>All versions prior to B3F</i>	
Easergy MiCOM P642, P645 <i>All versions prior to B4A</i>	
Easergy MiCOM P741, P742, P743 <i>All versions prior to B2A</i>	
Easergy MiCOM P746 <i>All versions prior to B4E or C4E</i>	
Easergy MiCOM P849 <i>All versions prior to B4A</i>	

Schneider Electric Security Notification

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](#) if you need assistance removing a patch.

To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here:

<https://www.se.com/en/work/support/cybersecurity/notification-contact.jsp>

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 intended for that device.
- 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.

For more information refer to the Schneider Electric [Recommended Cybersecurity Best Practices](#) document.

Schneider Electric Security Notification

Acknowledgements

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

CVE	Researcher
CVE-2026-4832	Anonymous

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, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services:

<https://www.se.com/ww/en/work/solutions/cybersecurity/>. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page: <https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH 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

Schneider's purpose is to **create Impact** by empowering all to **make the most of our energy and resources**, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be the trusted partner in **Sustainability and Efficiency**.

We are a **global industrial technology leader** bringing world-leading expertise in electrification, automation and digitization to smart **industries**, resilient **infrastructure**, future-proof **data centers**, intelligent **buildings**, and intuitive **homes**. Anchored by our deep

Schneider Electric Security Notification

domain expertise, we provide integrated end-to-end lifecycle AI enabled Industrial IoT solutions with connected products, automation, software and services, delivering digital twins to enable profitable growth **for our customers**.

We are a **people company** with an ecosystem of 150,000 colleagues and more than a million partners operating in over 100 countries to ensure proximity to our customers and stakeholders. We embrace **diversity and inclusion** in everything we do, guided by our meaningful purpose of a **sustainable future for all**.

www.se.com

Revision Control:

Version 1.0.0 14 April 2026	Original Release
Version 2.0.0 12 May 2026	Updated the risk associated with successful exploitation of this vulnerability and revised the remediation table to a mitigation table to emphasize that multiple mitigation options are available.