Schneider Electric Security Notification

Insufficient Entropy vulnerability on Multiple Products

12 May 2026

Overview

Schneider Electric is aware of a vulnerability in the following products:

The Easergy C5 is a scalable and interoperable bay controller, protection and merging unit for large and critical infrastructure electrical distribution systems.

The Easergy MiCOM P30 is a family of multifunction protection and control relays designed for medium, high and extra high voltage electrical networks.

The Easergy MiCOM P40 is a protection relay series for Medium Voltage, High Voltage and Extra High Voltage protection.

The Easergy MiCOM C264 is a modular and compact substation or bay controller, smart RTU and MV one box solution

The EcoStruxure™ Power Automation System Gateway (EPAS=GTW) is a scalable, interoperable, and rugged communication gateway that helps to remotely monitor and operate electrical processes

The EcoStruxure Power Automation System User Interface (EPAS-UI) product is an HMI SCADA designed for electrical networks and substations operations.

The EcoStruxure Power Automation System Intelligent Power Management System and Fast Load Shedding (iPMFLS) is a range of solutions designed to overcome size and performances constraints.

The EcoStruxure™ Power Operation (EPO) are an on-premises software offers that provides a single platform to monitor and control medium and lower power systems.

The PowerLogic™ P5 is a medium voltage protection relay.

The PowerLogic™ P7 is a protection and control platform designed for complex and advanced electrical network applications.

The PowerLogic™ T300 is a modular platform for medium voltage and low voltage public distribution network management.

The PowerLogic™ T500 is a control unit and RTU for substation automation.

The Saitel DP RTU is a modular platform for medium voltage and low voltage public distribution and transmission network management.

Schneider Electric Security Notification

The EasyLogic T150 (formerly Saitel DR RTU) is a field device, offering a solid and powerful platform for data acquisition, communication, automation and IED integration for distribution and transmission networks, generation sector and railway.

Failure to apply the fix provided below may risk session hijacking, which could result in malicious actors performing unauthorized operations within the affected system.

Affected Products and Versions

Product	Version
Easergy MiCOM C264	Versions D6.x all versions Versions D7.33 and prior
Easergy C5	Version 1.1.17 and prior
Easergy MiCOM P30	All MiCOM P30 devices with Advanced Cyber Security (module or feature) Easergy MiCOM P139 version prior to P139.678.700 Easergy MiCOM P437 version prior to P437.678.700 Easergy MiCOM P439 version prior to P439.678.700 Easergy MiCOM P532 version prior to P532.678.700 Easergy MiCOM P539 version prior to P539.678.700 Easergy MiCOM P631 version prior to P631.678.700 Easergy MiCOM P632 version prior to P632.678.700 Easergy MiCOM P633 version prior to P633.678.700 Easergy MiCOM P634 version prior to P634.678.700 Easergy MiCOM P633 version P633.680.700 only Easergy MiCOM P634 version P634.680.700 only Easergy MiCOM P138 version prior to P138.677.700 Easergy MiCOM P436 version prior to P436.677.701 Easergy MiCOM P438 version prior to P438.677.701 Easergy MiCOM P638 version prior to P638.677.700 Easergy MiCOM C434 version prior to C434.679.700
Easergy MiCOM P40	Easergy MiCOM P40 Series model numbers with Protocol Option bit as G, H or L and all firmware versions P_ 4_ _ _ _ _ G_ _ _ _ _ M P_ 4_ _ _ _ _ H_ _ _ _ _ M P_ 4_ _ _ _ _ L_ _ _ _ _ M P_ 4_ _ _ _ _ G_ _ _ _ _ L P_ 4_ _ _ _ _ H_ _ _ _ _ L P_ 4_ _ _ _ _ L_ _ _ _ _ L

EcoStruxure™ Power Automation System Gateway (EPAS-GTW)	Version 6.4.616.200.100 and prior
EcoStruxure Power Automation System User Interface (EPAS-UI)	Version 3.0.3 and prior
EcoStruxure™ Power Operation	Version 2022 CU6 and prior
EcoStruxure™ Power Operation	Version 2024 CU2 and prior
iPMFLS	Version 64.2025.0.13 and prior
PowerLogic™ P5 Protection Relay	V02.502.103 and prior
PowerLogic™ P7 Protection and Control Platform	V02.002.002 and prior
PowerLogic™ T300	Version 2.9.4 and prior
PowerLogic™ T500	Version 11.08.02 and prior
Saitel DP	Version 11.06.36 and prior
EasyLogic T150 (formerly Saitel DR)	Version 11.06.30 and prior

Vulnerability Details

CVE ID: **CVE-2026-4827**

CVSS v3.1 Base Score 8.3 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L
CVSS v4.0 Base Score 8.7 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N

CWE-331 Insufficient Entropy vulnerability exists that could lead to unauthorized access when an attacker on the network can exploit weaknesses in session-management protections.

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.

Remediation

Affected Product & Version	Remediation
Easergy MiCOM C264 *Versions D6.x all versions* *Version D7.33 and prior*	Version D7.34 of MiCOM C264 includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device. Reboot is required

Easergy C5 *Version 1.1.17 and prior*	Version 1.1.18 of Easergy C5 includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device. Reboot is required
Easergy MiCOM P30 *All MiCOM P30 devices with Advanced Cyber Security (module or feature)* *Easergy MiCOM P139 version prior to P139.678.700* *Easergy MiCOM P439 version prior to P439.678.700* *Easergy MiCOM P539 version prior to P539.678.700* *Easergy MiCOM P632 version prior to P632.678.700* *Easergy MiCOM P633 version prior to P633.678.700* *Easergy MiCOM P634 version prior to P634.678.700* *Easergy MiCOM P633 version P633.680.700 only* *Easergy MiCOM P138 version prior to P138.677.700* *Easergy MiCOM C434 version prior to C434.679.700*	Version P633.680.701 Easergy MiCOM P633 includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device. Version P539.678.700 Easergy MiCOM P539 includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device. Version P634.680.701 Easergy MiCOM P634 includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device. Version P139.678.700 Easergy MiCOM P139 includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device. Version P439.678.700 Easergy MiCOM P439 includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device. Version P138.677.701 Easergy MiCOM P138 includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device. Version C434.679.700 Easergy MiCOM C434 includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device. Version P632.678.700 Easergy MiCOM P632 includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device. Version P633.678.700 Easergy MiCOM P633 includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device.

EasyLogic T150 (formerly Saitel DR) *Version 11.06.30 and prior*	HUe Firmware version 11.06.31 includes a fix for this vulnerability and is available for download. Contact Schneider Electric's Customer Care Center to download this firmware. A reboot is needed to complete the firmware upgrade.
EcoStruxure™ Power Automation System Gateway *Version 6.4.616.200.100 and prior*	Version 6.4.610.500.101 of EPAS Gateway includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center to download this software.
EcoStruxure Power Automation System User Interface (EPAS-UI) *Version 3.0.3 and prior*	Version 3.0.4 of EPAS-UI includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center to download this software.
EcoStruxure™ Power Operation *EPO 2022 CU 6 and prior*	EPO 2022 CU 7 of EcoStruxure™ Power Operation includes a fix for this vulnerability and is available for download here: • https://community.se.com/t5/EcoStruxure-Power-Operation/Power-Operation-2022-CU7-is-Now-Available/td-p/524787 Reboot needed: yes
EcoStruxure™ Power Operation *EPO 2024 CU 2 and prior*	EPO 2024 CU 3 of EcoStruxure™ Power Operation includes a fix for this vulnerability and is available for download here: • https://community.se.com/t5/EcoStruxure-Power-Operation/Power-Operation-2024-CU3-is-HERE/td-p/534769 Reboot needed: yes
iPMFLS *Version 64.2025.0.13 and prior*	Version 64.2025.0.14 of iPMFLS includes a fix for this vulnerability. Contact Schneider Electric's Customer Care Center for information on how to contact your local Application Center to update the device.
PowerLogic™ P5 Protection Relay *V02.502.103 and prior*	Version V02.503.101 of PowerLogic™ P5 includes a fix for this vulnerability Contact Schneider Electric's Customer Care Center to download this firmware.
PowerLogic™ P7 Protection and Control Platform *V02.002.002 and prior*	Version V02.003.001 of PowerLogic™ P7 includes a fix for this vulnerability Contact Schneider Electric's Customer Care Center to download this firmware.
PowerLogic™ T300 *Version 2.9.4 and prior*	Version 2.9.5 of PowerLogic™ T300 includes a fix for this vulnerability Contact Schneider Electric's Customer Care Center to download this firmware. A reboot is needed to complete the firmware upgrade.
PowerLogic™ T500 *Version 11.08.02 and prior*	Version 11.08.03 of PowerLogic™ T500 includes a fix for this vulnerability Contact Schneider Electric's Customer Care Center to download this firmware. A reboot is needed to complete the firmware upgrade.

Saitel DP *Version 11.06.36 and prior*	CPU866e Firmware version 11.06.37 includes a fix for this vulnerability and is available for download. Contact Schneider Electric's Customer Care Center to download this firmware. A reboot is needed to complete the firmware upgrade.

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.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

Mitigations

Affected Product & Version	Mitigations
Easergy MiCOM P30 *All MiCOM P30 devices with Advanced Cyber Security (module or feature)* *Easergy MiCOM P437 version prior to P437.678.700* *Easergy MiCOM P532 version prior to P532.678.700* *Easergy MiCOM P631 version prior to P631.678.700* *Easergy MiCOM P634 version P634.680.700 only* *Easergy MiCOM P436 version prior to P436.677.701* *Easergy MiCOM P438 version prior to P438.677.701* *Easergy MiCOM P638 version prior to P638.677.700*	Schneider Electric is establishing a remediation plan for all future versions of the following models of the Easergy MiCOM P30: P437 P532 P631 P634 P436 P438 P638 Future versions will include a fix for this vulnerability. We will update this document when the remediation is available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit: • Ensure P30 operates within a physically or logically segmented internal network. Access to this network should be tightly controlled using standard security mechanisms such as firewalls, intrusion detection systems (IDS), and other relevant protective measures. • Reduce the "Minimum inactivity period" using the CAE tool to shorten session timeout durations and minimize the risk of unauthorized access due to inactive sessions.

Schneider Electric Security Notification

Easergy MiCOM P40 *Series model numbers with Protocol Option bit as G, H or L and all firmware versions* *P_ 4_ _ _ _ _ G_ _ _ _ _ M* *P_ 4_ _ _ _ _ H_ _ _ _ _ M* *P_ 4_ _ _ _ _ L_ _ _ _ _ M* *P_ 4_ _ _ _ _ G_ _ _ _ _ L* *P_ 4_ _ _ _ _ H_ _ _ _ _ L* *P_ 4_ _ _ _ _ L_ _ _ _ _ L*	Schneider Electric is establishing a remediation plan for a future version of the Easergy MiCOM P40 Series model numbers with Protocol Option bit as G, H or L. P_ 4_ _ _ _ _ G_ _ _ _ _ M P_ 4_ _ _ _ _ H_ _ _ _ _ M P_ 4_ _ _ _ _ L_ _ _ _ _ M P_ 4_ _ _ _ _ G_ _ _ _ _ L P_ 4_ _ _ _ _ H_ _ _ _ _ L P_ 4_ _ _ _ _ L_ _ _ _ _ L A future version will include a fix for this vulnerability. We will update this document when the remediation is available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit: • Ensure P40 operates within a physically or logically segmented internal network. Access to this network should be tightly controlled using standard security mechanisms such as firewalls, intrusion detection systems (IDS), and other relevant protective measures. • Reduce the “Minimum inactivity period” using the CAE tool to shorten session timeout durations and minimize the risk of unauthorized access due to inactive sessions.

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/security-notifications.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.

Acknowledgements

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

CVE	Researcher
CVE-2026-4827	Internal Schneider Electric Researcher

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

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.

Schneider Electric Security Notification

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 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 *12 May 2026*	Original Release

CPCERT

Digitally signed by CPCERT
Date: 2026.05.11 12:26:04 -05'00'