Schneider Electric Security Notification

Third-Party vulnerability on Modicon Networking Managed Switches

14 April 2026

Overview

Schneider Electric is aware of a RADIUS protocol vulnerability affecting its Modicon Network Managed Switch product.

The Modicon Network Managed Switch product provides connectivity for multiple Ethernet devices, network management, enhanced cyber security and more advanced switching features.

Failure to apply the mitigation provided below may risk forgery attacks in RADIUS Protocol, which could result in modification of any valid Response (Access-Accept, Access-Reject, or Access-Challenge) to any other response which could result in the possibility of denial of service and loss of confidentiality, integrity of the devices connected to the switch.

Affected Products and Versions

Product	Version
Connexium Managed Switches • TCSESM* Modicon Managed Switches • MCSESM*, MCSESP* Modicon Redundancy Switches • MCSESR*	All versions

Vulnerability Details

CVE ID: **CVE-2024-3596**

CVSS v3.1 Base Score 9.0 | Critical | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CWE-924 Improper Enforcement of Message Integrity During Transmission in a Communication Channel

Additional information about CVE-2024-3596 can be found here:

https://www.cve.org/CVERecord?id=CVE-2024-3596

Mitigations

Affected Product & Version	Mitigations
Connexium Managed Switches • TCSESM* Modicon Managed Switches • MCSESM*, MCSESP* Modicon Redundancy Switches • MCSESR* *All versions*	The default RADIUS configuration is **not** vulnerable. However, if the *RADIUS Server Message Authenticator* option is **disabled**, the product becomes vulnerable. We advise keeping this parameter in its default (enabled) state. This parameter can be configured via CLI and SNMP: **TCSESM*** CLI: radius server msgauth MIB: hmAgentRadiusServerMsgAuth **MCSESM*, MCSESP*** CLI: radius server auth modify <index> msgauth MIB: hm2AgentRadiusServerMsgAuth **MCSESR*** CLI: radius server auth modify <index> msgauth MIB: hm2AgentRadiusServerMsgAuth

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.

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.

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.**

Schneider Electric Security Notification

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

CPCERT

Digitally signed by CPCERT
Date: 2026.04.13 20:00:52 -05'00'