Schneider Electric Security Notification

Modicon Controllers M241/M251/M258/LMC058/M262

10 June 2025

Overview

Schneider Electric is aware of multiple vulnerabilities in its Modicon Controllers M241 / M251 / M258 / LMC058 / M262 products.

The Modicon Controllers M241/M251/M258/M262 and Modicon LMC058 products are Programmable Logic Controllers for performance-demanding applications.

Failure to apply remediation/mitigations provided below may risk Cross-Site Scripting, Denial of Service or uncontrolled resource consumption which could result in loss of confidentiality, integrity and availability of the controller.

Affected Products and Versions

Product	CVE-2025-3898	CVE-2025-3899 CVE-2025-3112	CVE-2025-3905 CVE-2025-3116	CVE-2025-3117
Modicon Controllers M241/M251	Versions prior to 5.3.12.51	Versions prior to 5.3.12.51	Versions prior to 5.3.12.51	Versions prior to 5.3.12.51
Modicon Controllers M262	Versions prior to 5.3.9.18	Not impacted	Not impacted	Versions prior to 5.3.9.18
Modicon Controllers M258 / LMC058	Not impacted	Not impacted	All versions	All versions

Vulnerability Details

CVE ID: **CVE-2025-3898**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score 7.1 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N
CWE-20: Improper Input Validation vulnerability exists that could cause Denial of Service when an authenticated malicious user sends HTTPS request containing invalid data type to the webserver.

CVE ID: **CVE-2025-3899**

CVSS v3.1 Base Score 5.4 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
CVSS v4.0 Base Score 5.1 | Medium | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists in Certificates page on Webserver that could cause an unvalidated data injected by authenticated malicious user leading to modify or read data in a victim’s browser.

CVE ID: **CVE-2025-3112**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score 7.1 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-400: Uncontrolled Resource Consumption vulnerability exists that could cause Denial of Service when an authenticated malicious user sends manipulated HTTPS Content-Length header to the webserver.

CVE ID: **CVE-2025-3905**

CVSS v3.1 Base Score 5.4 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
CVSS v4.0 Base Score 5.1 | Medium | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N

CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists impacting PLC system variables that could cause an unvalidated data injected by authenticated malicious user leading to modify or read data in a victim's browser.

CVE ID: **CVE-2025-3116**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
CVSS v4.0 Base Score 7.1 | High | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CWE-20: Improper Input Validation vulnerability exists that could cause Denial of Service when an authenticated malicious user sends special malformed HTTPS request containing improper formatted body data to the controller.

CVE ID: **CVE-2025-3117**

CVSS v3.1 Base Score 5.4 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N
CVSS v4.0 Base Score 5.1 | Medium | CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:P/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N
CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists impacting configuration file paths that could cause an unvalidated data injected by authenticated malicious user leading to modify or read data in a victim's browser.

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
Modicon Controllers M241/M251 *Versions prior to* 5.3.12.51	Version 5.3.12.51 of Modicon Controllers M241/M251 includes a fix for these vulnerabilities and can be downloaded here: https://www.se.com/ww/en/product-range/62129-modicon-m241-micro-plc/#software-and-firmware https://www.se.com/ww/en/product-range/62130-modicon-m251-micro-plc-with-dual-channel-comm/#software-and-firmware Use the Controller Assistant feature of EcoStruxure™ Automation Expert – Motion V24.1 -to update the M241/M251 firmware and perform a reboot. EcoStruxure™ Automation Expert – Motion V24.1 is available via the Schneider Electric Software Installer: https://www.se.com/ww/en/download/document/ESEMACS10_INSTALLER
Modicon Controllers M262 *Versions prior to 5.3.9.18*	Versions from 5.3.9.18 of Modicon Controllers M262 include a fix for these vulnerabilities and can be downloaded here: https://www.se.com/ww/en/product-range/65771-logic-motion-controller-modicon-m262/#software-and-firmware Use the Controller Assistant feature of EcoStruxure™ Automation Expert – Motion V24.1 to update the M262 firmware and perform a reboot. EcoStruxure™ Automation Expert – Motion V24.1 is available via the Schneider Electric Software Installer: https://www.se.com/ww/en/download/document/ESEMACS10_INSTALLER

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
Modicon Controllers M241/ M251 *Versions prior to* 5.3.12.51 **Modicon Controllers M262** *Versions prior to 5.3.9.18* **Modicon Controllers M258 / LMC058** *All versions*	Schneider Electric is establishing a remediation plan for all future versions of Modicon M258/LMC058 that 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: • Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from public internet or untrusted networks. • Ensure usage of user management and password features. User rights are enabled by default and forced to create a strong password at first use. • Deactivate the Webserver after use when not needed. • Use encrypted communication links. • Setup network segmentation and implement a firewall to block all unauthorized access to ports 80/HTTP and 443/HTTPS. • Use VPN (Virtual Private Networks) tunnels if remote access is required. • The "Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment" provide product specific hardening guidelines. 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 these vulnerabilities:

CVE	Researcher
CVE-2025-3898 CVE-2025-3899 CVE-2025-3112 CVE-2025-3905 CVE-2025-3116 CVE-2025-3117	Loc Nguyen (Unit 515, OPSWAT) Dat Phung (Unit 515, OPSWAT) Thai Do (Unit 515, OPSWAT) Minh Pham (Unit 515, OPSWAT)

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 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 10 June 2025	Original Release

CPCERT

Digitally signed by CPCERT
Date: 2025.06.09 10:57:06 -04'00'