America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS MEDICAL ADVISORY

Medtronic MyCareLink Patient Monitor (Update A)

Last Revised: May 07, 2026 **Alert Code:** ICSMA-25-205-01

RELATED TOPICS: INDUSTRIAL CONTROL SYSTEM VULNERABILITIES </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, INDUSTRIAL CONTROL SYSTEMS </topics/industrial-control-systems>

View CSAF <https://github.com/cisagov/csaf/blob/develop/csaf_files/ot/white/2025/icsma-25-205-01.json>

Summary

Successful exploitation of these vulnerabilities could lead to system compromise, unauthorized access to sensitive data, and manipulation of the monitor's functionality.

The following versions of Medtronic MyCareLink Patient Monitor (Update A) are affected:

- MyCareLink Patient Monitor model 24950 vers:all/* (CVE-2025-4394, CVE-2025-4395, CVE-2025-4393, CVE-2018-10622, CVE-2025-4386, CVE-2025-4397)
- MyCareLink Patient Monitor model 24952 vers:all/* (CVE-2025-4394, CVE-2025-4395, CVE-2025-4393, CVE-2018-10622, CVE-2025-4386, CVE-2025-4397)

CVSS	Vendor	Equipment	Vulnerabilities
v3 6.8	Medtronic	Medtronic MyCareLink Patient Monitor (Update A)	Cleartext Storage of Sensitive Information, Empty Password in Configuration File, Deserialization of Untrusted Data, Cleartext Storage in a File or on Disk, Improper Physical Access Control

Background

- **Critical Infrastructure Sectors:** Healthcare and Public Health
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** Ireland

Vulnerabilities

Expand All +

CVE-2025-4394 +

CVE-2025-4395 +

CVE-2025-4393 +

CVE-2018-10622 +

CVE-2025-4386 +

CVE-2025-4397 +

Acknowledgments

- Ethan Morchy of Somerset ReconCarl Mann reported these vulnerabilities to Medtronic
- An independent researcher reported these vulnerabilities to Medtronic

Legal Notice and Terms of Use

Recommended Practices

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on cisa.gov/ics. Several CISA products detailing cyber defense best practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing suspected malicious activity should follow established internal procedures and report findings to CISA for tracking and correlation against other incidents.

No known public exploitation specifically targeting these vulnerabilities has been reported to CISA at this time. These vulnerabilities are not exploitable remotely.

Revision History

- **Initial Release Date:** 2025-07-24

Date	Revision	Summary
2025-07-24	1	Initial Publication
2026-05-07	2	Update A

Legal Notice and Terms of Use

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Medtronic

Tags

Sector: Healthcare and Public Health Sector </topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector>

Topics: Industrial Control System Vulnerabilities </topics/industrial-control-systems/industrial-control-system-vulnerabilities>, Industrial Control Systems </topics/industrial-control-systems>

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Related Advisories

MAR 24, 2026 ■ ICS MEDICAL ADVISORY | ICSMA-26-083-01

Grassroots DICOM (GDCM) </news-events/ics-medical-advisories/icsma-26-083-01>

FEB 10, 2026 ■ ICS MEDICAL ADVISORY | ICSMA-26-041-01

ZOLL ePCR IOS Mobile Application </news-events/ics-medical-advisories/icsma-26-041-01>

DEC 30, 2025 ■ ICS MEDICAL ADVISORY | ICSMA-25-364-01

WHILL Model C2 Electric Wheelchairs and Model F Power Chairs (Update A) </news-events/ics-medical-advisories/icsma-25-364-01>

DEC 11, 2025 ■ ICS MEDICAL ADVISORY | ICSMA-25-345-01

Grassroots DICOM (GDCM) </news-events/ics-medical-advisories/icsma-25-345-01>

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov