America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS MEDICAL ADVISORY

Medtronic MyCareLink 24950 Patient Monitor (Update A)

Last Revised: May 07, 2026 **Alert Code:** ICSMA-18-219-01

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/2018/icsma-18-219-01.json>

Summary

Successful exploitation of these vulnerabilities may allow an attacker with physical access to obtain per-product credentials that are utilized to authenticate data uploads and encrypt data at rest. Additionally, an attacker with access to a set of these credentials and additional identifiers can upload invalid data to the Medtronic CareLink network.

The following versions of Medtronic MyCareLink 24950 Patient Monitor (Update A) are affected:

- 24950 MyCareLink Monitor vers:all/* (CVE-2018-10626, CVE-2018-10622)
- 24952 MyCareLink Monitor vers:all/* (CVE-2018-10626, CVE-2018-10622)

CVSS	Vendor	Equipment	Vulnerabilities
v3 6.8	Medtronic	Medtronic MyCareLink 24950 Patient Monitor (Update A)	Insufficient Verification of Data Authenticity, Cleartext Storage in a File or on Disk

Background

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

Vulnerabilities

Expand All +

CVE-2018-10626 +

CVE-2018-10622 +

Acknowledgments

- Billy Rios, Jesse Young, and Jonathan Butts of Whitescope LLC reported these vulnerabilities to CISA

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 have a high attack complexity.

Revision History

- **Initial Release Date:** 2018-08-07

Date	Revision	Summary
2018-08-07	1	Initial Publication
2026-05-07	2	Update A - Updated CVE-2018-10622 description and CVSS score and vector score.

Legal Notice and Terms of Use

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