America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS MEDICAL ADVISORY

Philips MRI 1.5T and 3T (Update A)

Last Revised: March 26, 2026 **Alert Code:** ICSMA-21-313-01

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/2021/icsma-21-313-01.json>

Summary

Successful exploitation of these vulnerabilities may allow an attacker with operator level access to view system configuration, view system files, and export data (including patient data) to an untrusted environment.

The following versions of Philips MRI 1.5T and 3T (Update A) are affected:

- MRI 1.5T >=5.3|<5.8.1
- MRI 3T >=5.3|<5.8.1

CVSS	Vendor	Equipment	Vulnerabilities
v3 6.2	Philips	Philips MRI 1.5T and 3T	Incorrect User Management, Incorrect Ownership Assignment, Files or Directories Accessible to External Parties

Background

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

Vulnerabilities

Expand All +

CVE-2021-26262 +

CVE-2021-26248 +

CVE-2021-42744 +

Acknowledgments

- Michael Aguilar of Secureworks Adversary Group reported these vulnerabilities to Philips

---

Legal Notice and Terms of Use

Recommended Practices

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities.

Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet.

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:** 2021-11-24

Date	Revision	Summary
2021-11-24	1	Initial Publication
2026-03-26	2	Update A - Updated Risk Evaluation, Affected versions updated to "5.3 to 5.8.1", CVSS

Legal Notice and Terms of Use

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

Vendor

- Philips

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

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

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

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-25-345-02

Varex Imaging Panoramic Dental Imaging Software </news-events/ics-medical-advisories/icsma-25-345-02>

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