America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ICS MEDICAL ADVISORY

MicroDicom DICOM Viewer

Release Date: May 01, 2025 **Alert Code:** ICSMA-25-121-01

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>

1. EXECUTIVE SUMMARY

- **CVSS v4 8.6**
- **ATTENTION**: Exploitable remotely/low attack complexity
- **Vendor**: MicroDicom
- **Equipment**: DICOM Viewer
- **Vulnerabilities**: Out-of-Bounds Write, Out-of-Bounds Read

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could allow an attacker to disclose information, cause memory corruption, and execute arbitrary code.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following MicroDicom products are affected:

- DICOM Viewer: Versions 2025.1 (Build 3321) and prior

3.2 VULNERABILITY OVERVIEW

3.2.1 OUT-OF-BOUNDS WRITE CWE-787

<https://cwe.mitre.org/data/definitions/787.html>

MicroDicom DICOM Viewer is vulnerable to an out-of-bounds write which may allow an attacker to execute arbitrary code. The user must open a malicious DCM file for exploitation.

CVE-2025-35975 has been assigned to this vulnerability. A CVSS v3.1 base score of 8.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.1#cvss:3.1/av:n/ac:l/pr:n/ui:r/s:u/c:h/i:h/a:h>).

A CVSS v4 score has also been calculated for CVE-2025-35975. A base score of 8.6 has been calculated; the CVSS vector string is (AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N <https://www.first.org/cvss/calculator/4.0#cvss:4.0/av:n/ac:l/at:n/pr:n/ui:a/vc:h/vi:h/va:h/sc:n/si:n/sa:n>).

3.2.2 OUT-OF-BOUNDS READ CWE-125

<https://cwe.mitre.org/data/definitions/125.html>

MicroDicom DICOM Viewer is vulnerable to an out-of-bounds read which may allow an attacker to cause memory corruption within the application. The user must open a malicious DCM file for exploitation.

CVE-2025-36521 has been assigned to this vulnerability. A CVSS v3.1 base score of 8.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.1#cvss:3.1/av:n/ac:l/pr:n/ui:r/s:u/c:h/i:h/a:h>).

A CVSS v4 score has also been calculated for CVE-2025-36521. A base score of 8.6 has been calculated; the CVSS vector string is (AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N <https://www.first.org/cvss/calculator/4.0#cvss:4.0/av:n/ac:l/at:n/pr:n/ui:a/vc:h/vi:h/va:h/sc:n/si:n/sa:n>).

3.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Healthcare and Public Health
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Bulgaria

3.4 RESEARCHER

Michael Heinzl reported these vulnerabilities to CISA.

4. MITIGATIONS

MicroDicom recommends user update DICOM Viewer to version 2025.2 <https://www.microdicom.com/downloads.html> or later.

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities, such as:

- Minimize network exposure for all control system devices and/or systems, ensuring they are not accessible from the internet <https://www.cisa.gov/uscert/ics/alerts/ics-alert-10-301-01>.
- Locate control system networks and remote devices behind firewalls and isolating them from business networks.
- When remote access is required, use more secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as the connected devices.

CISA recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. 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 <https://www.cisa.gov/resources-tools/resources/ics-recommended-practices> on the ICS webpage on cisa.gov/ics <https://www.cisa.gov/topics/industrial-control-systems>. 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 <https://us-cert.cisa.gov/sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

CISA encourages organizations to implement recommended cybersecurity strategies for proactive defense of ICS assets <https://www.cisa.gov/sites/default/files/publications/cybersecurity_best_practices_for_industrial_control_systems.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage at cisa.gov/ics <https://www.cisa.gov/topics/industrial-control-systems> in the technical information paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies <https://www.cisa.gov/uscert/ics/tips/ics-tip-12-146-01b>.

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

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open attachments in unsolicited email messages.
- Refer to Recognizing and Avoiding Email Scams <https://www.cisa.gov/uscert/sites/default/files/publications/emailscams0905.pdf> for more information on avoiding email scams.
- Refer to Avoiding Social Engineering and Phishing Attacks <https://www.cisa.gov/uscert/ncas/tips/st04-014> for more information on social engineering attacks.

No known public exploitation specifically targeting these vulnerabilities has been reported to CISA at this time.

5. UPDATE HISTORY

- May 1, 2025: Initial Publication

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'd welcome your feedback.

Related Advisories

APR 10, 2025 **ICS MEDICAL ADVISORY | ICSMA-25-100-01**

INFINITT Healthcare INFINITT PACS </news-events/ics-medical-advisories/icsma-25-100-01>

MAR 20, 2025 **ICS MEDICAL ADVISORY | ICSMA-25-079-01**

Santesoft Sante DICOM Viewer Pro </news-events/ics-medical-advisories/icsma-25-079-01>

MAR 13, 2025 **ICS MEDICAL ADVISORY | ICSMA-25-072-01**

Philips Intellispace Cardiovascular (ISCV) </news-events/ics-medical-advisories/icsma-25-072-01>

FEB 27, 2025 **ICS MEDICAL ADVISORY | ICSMA-25-058-01**

Dario Health USB-C Blood Glucose Monitoring System Starter Kit Android Application

</news-events/ics-medical-advisories/icsma-25-058-01>

Return to top

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

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

CISA Central

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