ICS MEDICAL ADVISORY

Medixant RadiAnt DICOM Viewer

Release Date: February 20, 2025 **Alert Code:** ICSMA-25-051-01

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 5.7**
- **ATTENTION**: Low attack complexity
- **Vendor**: Medixant
- **Equipment**: RadiAnt DICOM Viewer

- **Vulnerability**: Improper Certificate Validation

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to perform a machine-in-the-middle attack (MITM), resulting in malicious updates being delivered to the user.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following Medixant products are affected:

- RadiAnt DICOM Viewer: Version 2024.02

3.2 VULNERABILITY OVERVIEW

3.2.1 IMPROPER CERTIFICATE VALIDATION CWE-295

<https://cwe.mitre.org/data/definitions/295.html>

The affected product is vulnerable due to failure of the update mechanism to verify the update server's certificate which could allow an attacker to alter network traffic and carry out a machine-in-the-middle attack (MITM). An attacker could modify the server's response and deliver a malicious update to the user.

CVE-2025-1001 has been assigned to this vulnerability. A CVSS v3.1 base score of 5.7 has been calculated; the CVSS vector string is (AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N <https://www.first.org/cvss/calculator/3.1#cvss:3.1/av:a/ac:l/pr:n/ui:r/s:u/c:n/i:h/a:n>).

A CVSS v4 score has also been calculated for CVE-2025-1001. A base score of 5.7 has been calculated; the CVSS vector string is (AV:A/AC:L/AT:P/PR:N/UI:A/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N

<https://www.first.org/cvss/calculator/4.0#cvss:4.0/av:a/ac:l/at:p/pr:n/ui:a/vc:n/vi:h/va:n/sc:n/si:n/sa:n>).

3.3 BACKGROUND

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

3.4 RESEARCHER

Sharon Brizinov of Claroty Team82 reported this vulnerability to CISA.

4. MITIGATIONS

Medixant recommends users download the v2025.1 or later version <https://www.radiantviewer.com/files/radiant-2025.1-setup.exe> of their software.

If users are unable to update to the new version, Medixant recommends the following:

- Disable the display of available updates via this command reg add "HKCU\Software\RadiAnt Viewer" /t REG_DWORD /v CheckUpdate /d 0 /f.
- Do not check manually for updates ("Check for updates now" from the toolbar menu).
- Ignore any update notifications coming from RadiAnt DICOM Viewer, download the latest version directly in the web browser from https://www.radiantviewer.com <https://www.radiantviewer.com/>.
- Check the downloaded RadiAnt DICOM Viewer installation package with antivirus software before running it.

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability, 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 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 this vulnerability has been reported to CISA at this time. This vulnerability is not exploitable remotely.

5. UPDATE HISTORY

- February 20, 2025: Initial Publication

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

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

FEB 13, 2025 ICS MEDICAL ADVISORY | ICSMA-25-044-01

Qardio Heart Health IOS and Android Application and QardioARM A100 </news-events/ics-medical-advisories/icsma-25-044-01>

FEB 06, 2025 ICS MEDICAL ADVISORY | ICSMA-25-037-01

MicroDicom DICOM Viewer </news-events/ics-medical-advisories/icsma-25-037-01>

FEB 06, 2025 ICS MEDICAL ADVISORY | ICSMA-25-037-02

Orthanc Server </news-events/ics-medical-advisories/icsma-25-037-02>

JAN 30, 2025 ICS MEDICAL ADVISORY | ICSMA-25-030-01

Contec Health CMS8000 Patient Monitor </news-events/ics-medical-advisories/icsma-25-030-01>

Return to top