

Forum:[Hack Forums](#)

Thread: [ZOLL ePCR IOS Mobile Application](#)

Stanley - February 21, 2026, 7:05 am

ZOLL ePCR IOS Mobile Application

View CSAF

Summary

Successful exploitation of this vulnerability could allow an attacker to gain unauthorized access to protected health information (PHI) or device telemetry.

The following versions of ZOLL ePCR IOS Mobile Application are affected:

ePCR IOS Mobile Application 2.6.7 (CVE-2025-12699)

CVSS

Vendor

Equipment

Vulnerabilities

v3 5.5

ZOLL

ZOLL ePCR IOS Mobile Application

Insertion of Sensitive Information into Externally-Accessible File or Directory

Background

Critical Infrastructure Sectors: Healthcare and Public Health

Countries/Areas Deployed: Worldwide

Company Headquarters Location: United States

Vulnerabilities

Expand All +

CVE-2025-12699

The ZOLL ePCR IOS application reflects unsanitized user input into a WebView. Attacker-controlled strings placed into PCR fields (run number, incident, call sign, notes) are interpreted as HTML/JS

when the app prints or renders that content. In the proof of concept (POC), injected scripts return local file content, which would allow arbitrary local file reads from the app's runtime context. These local files contain device and user data within the ePCR medical application, and if exposed, would allow an attacker to access protected health information (PHI) or device telemetry.

[View CVE Details](#)

Affected Products

ZOLL ePCR IOS Mobile Application

Vendor:ZOLL

Product Version:ZOLL ePCR IOS Mobile Application: 2.6.7

Product Status:known_affected

Remediations

MitigationZOLL ePCR IOS application was decommissioned in May 2025. ZOLL has no current plans to provide a replacement application. If users have questions or concerns, they are encouraged to reach out directly to ZOLL Support. <https://www.zolldata.com/contact-us>.

Relevant CWE: CWE-538 Insertion of Sensitive Information into Externally-Accessible File or Directory

Metrics

CVSS Version

Base Score

Base Severity

Vector String

3.1

5.5

MEDIUM

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

Acknowledgments

Bryan Riggins reported this vulnerability to ZOLL

Legal Notice and Terms of Use

This product is provided subject to this Notification (<https://www.cisa.gov/notification>) and this Privacy & Use policy (<https://www.cisa.gov/privacy-policy>).

Recommended Practices

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.

- 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 on the ICS webpage on [cisa.gov/ics](https://www.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](https://www.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.

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 for more information on avoiding email scams.

- Refer to Avoiding Social Engineering and Phishing Attacks 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.

Revision History

Initial Release Date: 2026-02-10

Date

Revision

Summary

2026-02-10

1

Initial Publication

Legal Notice and Terms of Use

<https://www.cisa.gov/news-events/ics-medical-advisories/icsma-26-041-01>