Penetration Test Report

CardioSense SaMD Application Security Assessment

Report Reference: PT-2026-001
Test Date: 2026-01-08 to 2026-01-12
Testing Firm: SecureHealth Consulting Ltd
Lead Tester: Dr. Marcus Webb, OSCP, CISSP
Application: CardioSense v2.1.0 (SaMD Class C)
Scope: Web API, Mobile App, Cloud Infrastructure
Classification: Confidential - Restricted Distribution

1. Executive Summary

SecureHealth Consulting performed a comprehensive penetration test of the CardioSense SaMD application. Testing covered OWASP Top 10, API security, authentication/authorization, data encryption, and cloud infrastructure configuration. Testing was performed against the staging environment which mirrors production configuration.

Overall Risk Rating: LOW. No critical or high-severity vulnerabilities were identified. Three medium-severity and five low-severity findings were documented.

2. Findings Summary

Severity	ID	Description
MEDIUM	PT-F001	Missing rate limiting on /api/auth/login endpoint
MEDIUM	PT-F002	Session token not rotated after privilege change
MEDIUM	PT-F003	Verbose error messages expose stack traces in staging
LOW	PT-F004	Missing Content-Security-Policy header on web app
LOW	PT-F005	X-Powered-By header reveals server technology
LOW	PT-F006	Autocomplete not disabled on sensitive form fields
LOW	PT-F007	Cookie missing SameSite=Strict attribute
LOW	PT-F008	DNS CAA records not configured

3. Detailed Findings

PT-F001: Missing Rate Limiting (Medium)

The /api/auth/login endpoint does not enforce rate limiting, allowing an attacker to perform brute-force attacks. Recommendation: Implement rate limiting of 5 attempts per minute with exponential backoff.

PT-F002: Session Token Rotation (Medium)

After a user changes their role or permissions, the session token is not regenerated. Recommendation: Rotate session tokens after any privilege change to prevent session fixation attacks.

PT-F003: Verbose Error Messages (Medium)

API error responses include full stack traces in the staging environment. Recommendation: Ensure production builds strip stack traces from error responses. Verify this is not the case in production deployment.

4. Conclusion & Recommendations

The CardioSense application demonstrates a strong security posture overall. No critical vulnerabilities were identified that would allow unauthorized access to patient data or medical device functionality. The medium-severity findings should be addressed within 30 days. Low-severity findings should be addressed within the next release cycle.

The application meets the security requirements specified in IEC 62443 and the FDA Guidance on Cybersecurity for Medical Devices (2023).

Dr. Marcus Webb, OSCP, CISSP
Principal Security Consultant
SecureHealth Consulting Ltd
Date: 2026-01-15