Diagnosing the security of the Massachusetts Health Insurance Exchange

AT A GLANCE

The Massachusetts Health Insurance Exchange (MA HIX) System provides an Integrated Eligibility System (IES) that was developed to enable the State of Massachusetts to comply with the Affordable Care Act (ACA). Since the state-of-the-art system crossed public and commercial markets, ensuring that the data and system were operationally secure was critical.

CLIENT CHALLENGE

The Massachusetts Office of Information Technology (MassIT) needed to evaluate if required controls were in place for the MA HIX. Coalfire was hired to perform the Federal Information Security Management Act (FISMA) assessment to determine compliance with the Centers for Medicare & Medicaid Services' (CMS) control objectives.

APPROACH

Coalfire performed the assessment in accordance with the model outlined in the CMS Acceptable Risk Safeguards (ARS) and National Institute of Standards and Technology (NIST) Special Pub (SP) 800-53A, Guide for Assessing the Security Controls in Federal Information Systems. Controls were assessed based on the CMS Minimum Security Requirements (CMSR), Appendix B CMSR Moderate Impact Level Data.

Vulnerability assessment methodology

Using a variety of discovery and vulnerability assessment tools, Coalfire assessors gathered and classified systems, open ports, running services, and vulnerabilities detected within the target environment. The frequency and significance of the vulnerabilities identified were analyzed to determine enterprise-level architectural and programmatic recommendations. The types of vulnerabilities processed were:

- Remote code execution
- Weak configurations
- Susceptibility to malware
- Patch level enumeration
- Use of insecure services and protocols
- Database server vulnerabilities
- Web server vulnerabilities

Penetration testing methodology

Vulnerability findings were then considered for use in penetration testing. Coalfire's advanced application penetration tests were executed to find vulnerabilities that could be exploited to compromise the application and data in transit, process, or stores.

Penetration testing scenarios included:

- Code injection
- Broken authentication session management
- Cross site scripting (XSS)
- Insecure direct object references
- Security misconfiguration
- Sensitive data exposure
- Missing function level access control
- Cross site request forgery (CSRF)
- Using components with known vulnerabilities
- Invalidated redirects and forwards

RESULTS

Through Coalfire's efforts the MA HIX met the ACA deadline in offering healthcare options to citizens. Data processed by the exchange is secure, and privacy for healthcare and participatory data is assured.

Coalfire's assessment deliverables contained a detailed report on vulnerabilities including risk ratings and recommendations for remediation at the system, architectural, and security program levels. Coalfire also provided briefings to discuss the findings and remediation with state executives and stakeholders.

CS_FISMA_Massachusetts_050117

COALFIRE

About Coalfire

As cybersecurity risk management and compliance experts, Coalfire delivers cybersecurity advice, assessments, testing, and implementation support to IT and security departments, executives, and corporate directors of leading enterprises and public sector organizations. By addressing each organization's specific challenges, we're able to develop a long-term strategy that improves our clients' overall cyber risk profiles. Armed with our trusted insights, clients can get to market faster with the security to succeed. Coalfire has offices throughout the United States and Europe. **Coalfire.com**