Report in Brief
Date: March 2024
Report No. A-18-22-09010

U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES
OFFICE OF INSPECTOR GENERAL

Alabama MMIS and E&E System Security Controls Were Adequate, but Some Improvements Are Needed

Why OIG Did This Audit

We are conducting a series of audits of State Medicaid Management Information Systems (MMISs) and Eligibility and Enrollment (E&E) systems of selected States to determine how well these systems are protected when subjected to cyberattacks.

Our objectives were to determine: (1) whether security controls in operation for Alabama MMIS and E&E system environments were effective in preventing certain cyberattacks, (2) the likely level of sophistication or complexity an attacker needs to compromise Alabama's MMIS and E&E system or its data, and (3) Alabama's ability to detect cyberattacks against its MMIS and E&E system and respond appropriately.

How OIG Did This Audit

We conducted a penetration test of the Alabama MMIS and E&E system from November through December 2022. The penetration test focused on the MMIS and E&E system's public IP addresses and web application URLs. We also conducted a simulated phishing campaign that included Alabama personnel in December 2022. We contracted with XOR Security, LLC (XOR), to assist in conducting the penetration test. We closely oversaw the work performed by XOR, and the assessment was performed in accordance with agreed upon Rules of Engagement among OIG, XOR, and Alabama.

What OIG Found

The Alabama MMIS and E&E system had adequate security controls in place to prevent our simulated cyberattacks from resulting in a successful compromise; however, we found six security controls required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, that could be improved to better prevent certain cyberattacks.

In addition, we estimated that an adversary would need a moderate level of sophistication to compromise the Alabama MMIS and E&E system. Finally, Alabama demonstrated that it has implemented adequate controls to detect and block phishing emails sent from a known malicious IP address. However, improvements to its detection controls are needed to better identify certain web application cyberattacks.

Alabama did not effectively implement some security controls because, in part, its vulnerability scanning tools did not identify the flaws and vulnerabilities we discovered in its systems. Additionally, Alabama did not adequately follow secure coding practices during their software development lifecycle and remediate vulnerabilities before deployment to Alabama's production systems. As a result of Alabama not effectively implementing security controls or identifying vulnerabilities, an attacker could potentially launch certain cyberattacks against the Alabama MMIS and E&E system to remotely execute malicious code on a computer or redirect users to malicious websites. Such cyberattacks could facilitate an attacker's ability to get initial unauthorized access to an Alabama system and potentially allow them to move deeper into the network and/or extract sensitive information such as Personal Health Information.

What OIG Recommends and Alabama Comments

We made a series of recommendations for Alabama to improve its security controls over its MMIS and E&E system, including that it require its developers to follow secure coding best practice requirements.

Alabama concurred with our recommendations and stated that it has mitigated or has developed plans to mitigate the findings we identified. Although we have not yet confirmed the changes Alabama described in its comments, we commend Alabama for its ongoing efforts to improve the overall security posture of its MMIS and E&E system environments.

The full report can be found on the OIG website