Report in Brief
Date: May 2023
Report No. A-18-20-08001

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

The Centers for Medicare & Medicaid Services Should Improve Preventative and Detective Controls To More Effectively Mitigate the Risk of Compromise

Why OIG Did This Audit

We conducted a cyber threat hunt assessment of the Centers for Medicare & Medicaid Services' (CMS's) information systems to independently assess the effectiveness of CMS's cybersecurity defenses, identify potential indicators of compromise, determine whether any breaches have gone undetected, and review its incident response capabilities.

Our objectives were to determine whether: (1) CMS's cybersecurity defenses were effective, (2) there were active threats on the CMS network or whether there had been a past cyber breach, and (3) CMS was able to detect breaches and respond appropriately.

How OIG Did This Audit

We performed the cyber threat hunt of CMS's endpoints from August through November 2020. The assessment was performed on approximately 8,400 endpoints that CMS manages. We contracted with Accenture Federal Services (AFS) to conduct the cyber threat hunt of CMS. AFS provided subject matter experts during the initial planning, preparation, technology deployment, and discovery phases of the cyber threat hunt. OIG IT auditors completed the cyber hunt analysis and reporting phases of the cyber threat hunt. The assessment was performed in accordance with generally accepted government auditing standards and agreed-upon rules of engagement between OIG, AFS, and CMS.

What OIG Found

Although CMS had implemented some security controls for detecting and preventing threats on its network, CMS's cybersecurity controls needed improvements to better detect and prevent cyber threats on its network. We found multiple security controls at CMS that were not operating effectively, including controls related to monitoring and controlling communications at the CMS boundary, configurations to provide only essential capabilities, and controlling and preventing the installation of unauthorized software by users. Although we did not identify evidence of a past breach, we found one active and one potential threat to the CMS network. We promptly shared these findings with CMS during our audit period. Lastly, we concluded that CMS did not consistently detect threat activity that could lead to a potential breach. Specifically, CMS did not identify an active threat and other control weaknesses we found during the audit. Because we did not identify a breach within CMS's network, we have no opinion about CMS's ability to respond appropriately to a breach.

The security control failures that we identified occurred because CMS did not effectively align some of its security controls with their security policies or with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, requirements. For certain controls, CMS did not establish effective policies and procedures to periodically assess whether these controls were in place and operating effectively in accordance with the most current NIST SP 800-53 controls. As a result, cyber threat actors may have been able to successfully carry out a cyberattack or insiders may have been able to bypass CMS security controls that would allow them to exfiltrate sensitive data or allow the attacks to go undetected.

What OIG Recommends and CMS Comments

We recommend that CMS: (1) remediate the seven security control findings OIG identified, (2) update security controls to align with the most current NIST SP 800-53 requirements, and (3) enhance policies and procedures to periodically identify and assess whether security controls are in place and operating effectively in accordance with the most current NIST SP 800-53 controls and remediate weak controls timely. In written comments on our draft report, CMS concurred with all recommendations and described the actions it has taken. CMS disagreed with our assertion that scanning attempts of a web server represented an active threat on the CMS network. We agreed with CMS and made changes to the report accordingly. However, we consider the external scans a potential threat that could adversely impact organizational operations or assets because they provide valuable information about vulnerabilities to potential attackers that they can exploit.