Report in Brief
Date: June 2022
Report No. A-18-20-06500

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

The Centers for Medicare & Medicaid Services Had Policies and Procedures in Place To Mitigate Vulnerabilities in a Timely Manner, but Improvements Are Needed

Why OIG Did This Audit

Effective April 29, 2019, the Department of Homeland Security's Binding Operational Directive 19-02 (BOD 19-02) requires Federal agencies to remediate known "critical" vulnerabilities within 15 days of discovery and "high" vulnerabilities within 30 days of discovery. We have identified through previous oversight work that the Department of Health and Human Services has not always complied with BOD 19-02.

The cybersecurity community has adopted use of the Common Vulnerabilities and Exposure (CVE) list, which provides public information about vulnerabilities and the ways that they can be exploited. Malicious actors can research the CVE list and tailor attacks to systems that may be vulnerable if a security patch or update has not been implemented.

Our objective was to determine whether CMS had controls in place to remediate known cybersecurity vulnerabilities in accordance with Federal regulations.

How OIG Did This Audit

We reviewed CMS's policies and procedures for flaw remediation, interviewed CMS officials, and reviewed system security plans to determine whether CMS's flaw remediation controls were adequate.

What OIG Found

CMS had controls in place to remediate known vulnerabilities in accordance with Federal regulations and standards; however, it did not consistently apply security updates to systems with known vulnerabilities and did not consistently upgrade or patch operating systems that had reached the end of life period and were no longer supported by the vendor. This occurred because CMS did not have effective management oversight to ensure that CMS mitigated vulnerabilities in a timely manner. As a result, some CMS systems had open vulnerabilities that were vulnerable to exploitation by malicious actors beyond the acceptable limits defined in the BOD.

What OIG Recommends and CMS' Comments

We recommend that CMS: (1) remediate the vulnerabilities identified on internet-facing systems and implement procedures to ensure compliance with BOD 19-02 requirements; (2) implement procedures to ensure that unsupported software that no longer receives security updates, repairs, bug fixes, and threat mitigation is replaced prior to the known EOS or implement compensating controls (if possible) and accept risk in accordance with existing CMS policies and procedures; (3) implement oversight to ensure corrective actions are performed in accordance with Federal requirements and in the timeframe set forth in CMS policy; and (4) implement a process to centralize the monitoring and reporting of vulnerabilities identified in all CMS systems across all CMS data centers.

CMS concurred with all our recommendations and provided supporting documentation to remediate the technical vulnerabilities identified.