Report in Brief

August 16, 2021

Background

Beginning on January 11, 2020, servers operated by the U.S. Census Bureau (the Bureau) were attacked using a publicly available exploit. The purpose of these servers was to provide the Bureau with remote-access capabilities for its enterprise staff to access the production, development, and lab networks. According to system personnel, these servers did not provide access to 2020 decennial census networks. The exploit was partially successful, in that the attacker modified user account data on the systems to prepare for remote code execution. However, the attacker's attempts to maintain access to the system by creating a backdoor into the affected servers were unsuccessful.

The Enterprise Security Operations Center (ESOC) is the U.S. Department of Commerce's (the Department's) primary point of contact for reporting computer security incidents within the Department and to external stakeholders. During this incident, ESOC was responsible for facilitating information sharing between the Bureau and the U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Additionally, the Bureau's Computer Incident Response Team was responsible for responding to the incident.

Why We Did This Review

The objective of this audit was to assess the adequacy of the Bureau's process to respond to cybersecurity incidents according to federal and Departmental requirements.

U.S. CENSUS BUREAU

The U.S. Census Bureau's Mishandling of a January 2020 Cybersecurity Incident Demonstrated Opportunities for Improvement

OIG-21-034-A

WHAT WE FOUND

We found that the Bureau should make improvements to its cyber incident response process. Specifically, the Bureau missed opportunities to mitigate a critical vulnerability, which resulted in the exploitation of vital servers. Once the servers had been exploited, the Bureau did not discover and report the incident in a timely manner. Additionally, the Bureau did not maintain sufficient system logs, which hindered the incident investigation. Following the incident, the Bureau did not conduct a lessons-learned session to identify improvement opportunities. We also found that the Bureau was operating servers that were no longer supported by the vendor.

WHAT WE RECOMMEND

We recommend that the Director of the U.S. Census Bureau ensure that the Bureau's Chief Information Officer does the following:

1. Implement procedures to promptly notify relevant system personnel when critical vulnerabilities are publicly released.
2. Frequently review and update vulnerability scanning lists to ensure all network-addressable information technology (IT) assets are identified for vulnerability scanning, and document all exceptions as part of this process.
3. Ensure all network-addressable IT assets are scanned using credentials when feasible according to Bureau-determined frequencies, but no less than DHS's *Continuous Diagnostics and Mitigation Program* guidance.
4. Review the automated alert capabilities of the Bureau's security information and event management tool to ensure a similar attack can be identified in the future.
5. Ensure Bureau incident responders comply with Departmental and Bureau requirements to report confirmed computer security incidents to ESOC within 1 hour.

We recommend that the Deputy Secretary of the Department of Commerce ensure that the Department's Chief Information Officer does the following:

6. Develop ESOC procedures for the handling of alerts from outside entities (e.g., DHS CISA) to ensure information is conveyed to Department operating units in a timely manner.

We recommend that the Director of the U.S. Census Bureau ensure that the Bureau's Chief Information Officer does the following:

7. Incorporate periodic reviews of the Bureau's system log aggregation configurations to ensure all network-addressable IT assets are correctly configured.
8. Update Bureau incident response policies to include a specific timeframe prescribing when to conduct a review of lessons learned.
9. Establish plans with milestones to prioritize the decommissioning of end-of-life products.