Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

PENETRATION TEST OF THE FOOD AND DRUG ADMINISTRATION'S COMPUTER NETWORK

Inquiries about this report may be addressed to the Office of Public Affairs at Public.Affairs@oig.hhs.gov.

Thomas M. Salmon
Assistant Inspector General
for Audit Services

October 2014
A-18-13-30331

Office of Inspector General

http://oig.hhs.gov

The mission of the Office of Inspector General (OIG), as mandated by Public Law 95-452, as amended, is to protect the integrity of the Department of Health and Human Services (HHS) programs, as well as the health and welfare of beneficiaries served by those programs. This statutory mission is carried out through a nationwide network of audits, investigations, and inspections conducted by the following operating components:

Office of Audit Services

The Office of Audit Services (OAS) provides auditing services for HHS, either by conducting audits with its own audit resources or by overseeing audit work done by others. Audits examine the performance of HHS programs and/or its grantees and contractors in carrying out their respective responsibilities and are intended to provide independent assessments of HHS programs and operations. These assessments help reduce waste, abuse, and mismanagement and promote economy and efficiency throughout HHS.

Office of Evaluation and Inspections

The Office of Evaluation and Inspections (OEI) conducts national evaluations to provide HHS, Congress, and the public with timely, useful, and reliable information on significant issues. These evaluations focus on preventing fraud, waste, or abuse and promoting economy, efficiency, and effectiveness of departmental programs. To promote impact, OEI reports also present practical recommendations for improving program operations.

Office of Investigations

The Office of Investigations (OI) conducts criminal, civil, and administrative investigations of fraud and misconduct related to HHS programs, operations, and beneficiaries. With investigators working in all 50 States and the District of Columbia, OI utilizes its resources by actively coordinating with the Department of Justice and other Federal, State, and local law enforcement authorities. The investigative efforts of OI often lead to criminal convictions, administrative sanctions, and/or civil monetary penalties.

Office of Counsel to the Inspector General

The Office of Counsel to the Inspector General (OCIG) provides general legal services to OIG, rendering advice and opinions on HHS programs and operations and providing all legal support for OIG's internal operations. OCIG represents OIG in all civil and administrative fraud and abuse cases involving HHS programs, including False Claims Act, program exclusion, and civil monetary penalty cases. In connection with these cases, OCIG also negotiates and monitors corporate integrity agreements. OCIG renders advisory opinions, issues compliance program guidance, publishes fraud alerts, and provides other guidance to the health care industry concerning the anti-kickback statute and other OIG enforcement authorities.

The Food and Drug Administration needed to address cyber vulnerabilities on its computer network that could potentially have led to a data breach.

INTRODUCTION

This report provides an overview of the results of our penetration test of the Food and Drug Administration's (FDA) computer network. It does not include specific details of the vulnerabilities that we identified because of the sensitive nature of the information. We provided more detailed information and recommendations to FDA so that it could address the issues we identified.

WHY WE DID THIS REVIEW

Computer hackers are increasingly compromising Government systems, publishing sensitive data, and using stolen data to commit fraud. Threats to Federal agency Web applications are continually changing because of advances made by hackers, the release of new technology, and the deployment of increasingly complex systems. Web sites that are not properly secured are vulnerable to unauthorized users who could compromise the confidentiality of sensitive information or negatively affect the operations of Federal agencies.

The objective of this review was to determine whether the FDA's network and external Web applications were vulnerable to compromise through cyber attacks.

BACKGROUND

Penetration tests identify methods of gaining access to a system by using tools and techniques that attackers use. The objective of penetration testing is to uncover potential vulnerabilities in information technology (IT) products and information systems resulting from implementation errors, configuration faults, or other operational deployment weaknesses or deficiencies. This audit is one of a series of Office of Inspector General (OIG) audits using penetration testing on networks run by the U.S. Department of Health and Human Services (HHS) and its operating divisions.

FDA is responsible for protecting public health by assuring the safety, efficacy, and security of human and veterinary drugs, biological products, medical devices, our nation's food supply, cosmetics, and products that emit radiation. FDA is also responsible for advancing the public health by helping to speed innovations that make medicines more effective, safe, and affordable and for regulating the manufacturing, marketing, and distribution of tobacco products to protect public health and reduce tobacco use by minors.

FDA's Office of Information Management manages the IT infrastructure and ensures that FDA has a robust IT foundation that enables interoperability across FDA offices and allows development of enterprisewide systems that are necessary to meet FDA's mission efficiently and effectively. FDA's IT budget for fiscal year 2014 was $486 million, which was approximately 11 percent of the total FDA budget of $4.4 billion in fiscal year 2014, a significant investment.

On October 15, 2013 (before our fieldwork), a wide-scale cyber security breach involving an FDA system occurred that exposed sensitive information in 14,000 user accounts.

HOW WE CONDUCTED THIS REVIEW

We assessed the FDA network's exposure to cyber attacks by performing a penetration test of its network and information systems. We conducted the penetration test from October 21, 2013, through November 10, 2013, with the knowledge and permission of FDA officials. We requested that FDA's incident response staff not be notified of our testing to assess the effectiveness of FDA's intrusion detection and response controls. The Appendix contains the details of our audit scope and methodology.

FINDINGS

Overall, FDA needed to address cyber vulnerabilities on its computer network. Although we did not obtain unauthorized access to the FDA network, we identified the following issues: Web page input validation was inadequate, external systems did not enforce account lockout procedures, security assessments were not performed on all external servers, error messages revealed sensitive system information, and demonstration programs revealed sensitive information. These could have led to: (1) the unauthorized disclosure or modification of FDA data or (2) FDA mission-critical systems being made unavailable.

INADEQUATE WEB PAGE INPUT VALIDATION

Federal information systems should check the validity of information inputs to ensure that they are acceptable in terms of format and content.[1] Input validation helps to ensure the accuracy of user-supplied data and to prevent input attacks, such as reflected cross-site scripting.[2]

We identified FDA Web pages that did not perform adequate input validation on data entered by the user. Exploitation of this vulnerability could result in malicious input being sent from an attacker to FDA Web pages to hijack a user's Web browser application, install malicious programs, or redirect users to malicious Web pages.

EXTERNAL SYSTEMS DID NOT ENFORCE ACCOUNT LOCKOUT

Federal information systems are required to enforce a defined limit of consecutive invalid logon attempts by a user and automatically lock the account for a predetermined time period or until the account is released by an administrator.[3]

[1] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* Control SI-10.

[2] Reflected cross-site scripting occurs when a dynamically generated Web page takes untrusted data and returns them to be rendered within the victim's browser without proper validation and sanitization.

[3] NIST SP 800-53 Revision 4, Control AC-7.

We identified FDA external systems that did not enforce account lockout after repeated failed log-in attempts. An attacker could repeatedly attempt, either manually or using automated mechanisms, to gain access to an external system by entering a correct login name and password. If an attacker manages to authenticate to a system as an administrative user, he or she would gain control of the system and its content.

ASSESSMENTS WERE NOT PERFORMED ON ALL EXTERNAL SERVERS

The *HHS Office of the Chief Information Officer's Policy for Information Systems Security and Privacy Handbook* (PISSP Handbook) requires HHS's operating divisions to assess the security controls in information systems annually to determine the extent to which the controls are implemented correctly, operating as intended, and meeting the security requirements for the system. Additionally, the PISSP Handbook requires that all Department systems, hosted applications, and networks undergo periodic vulnerability scanning no less than annually.

Although we were allowed to test the majority of FDA's external Web applications, we did not perform penetration testing on seven external systems. FDA officials considered these systems to be mission critical and did not want to accept the risk of having them go offline. Hence, we could not verify whether security vulnerabilities existed within these systems and whether the vulnerabilities could be exploited to gain unauthorized access to FDA systems and data.

We asked to review reports for any security testing performed by FDA or a third-party organization for the seven external systems we did not test; however, we determined that FDA had performed a security assessment for only one of those seven systems. We reviewed the security assessment results, scope, and methodology for this system and determined that because the system was tested within a preproduction environment only, the security assessor was not able to validate FDA's claims that controls within the preproduction environment mirrored the production environment.[4] Therefore, there is a risk that vulnerabilities may exist within the production version of the system.

ERROR MESSAGES REVEALED SENSITIVE SYSTEM INFORMATION

Applications frequently generate error messages and display them to users. Many times these error messages are quite useful to attackers because the messages reveal application code or information that helps attackers exploit vulnerabilities. NIST requires Federal information systems to generate error messages that provide information necessary for corrective action without revealing information that could be exploited by adversaries.[5]

We identified FDA Web sites in which detailed error messages revealed sensitive system information. An attacker could use information obtained from detailed error messages, such as

[4] A review of FDA's configuration management controls for development, test, and operational environments was outside the scope of this audit.

[5] NIST SP 800-53 Revision 4, Control SI-11.

software version information, to launch specific attacks against FDA systems. Detailed error messages can help attackers pinpoint vulnerabilities to focus their attacks.

DEMONSTRATION PROGRAMS REVEALED SENSITIVE INFORMATION

Federal information systems should be configured to provide essential capabilities and to determine what functions and services, some of which are provided by default, should be disabled or even eliminated.[6] Oftentimes, software may leave demonstration programs or sample scripts available as part of a default installation.

We identified demonstration programs that could be run on FDA systems. The programs revealed sensitive internal system environment settings. Disclosure of such information could help an attacker to launch specific attacks against the FDA systems.

RECOMMENDATIONS

We made seven recommendations to FDA to address the security vulnerabilities that we identified. In general, we recommended that FDA fix the Web vulnerabilities identified, implement more effective procedures to protect its computer systems from cyber attacks, and periodically assess the security of all of its Internet-facing systems. This report summarizes our recommendations because of the sensitive nature of the information. We provided more detailed recommendations to FDA.

AUDITEE COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

In written comments to our draft report, FDA indicated that our findings have been addressed by the system owner(s) and remediation actions have been appropriately applied. We have not verified these actions because they took place after our audit period.

Implementation of our recommendations should further strengthen the information security of FDA's network and external Web applications. The timely implementation of our recommendations is important, and we plan to follow up with FDA on these audit results and its remediation actions.

[6] NIST SP 800-53 Revision 4, Control CM-7.

APPENDIX: AUDIT SCOPE AND METHODOLOGY

SCOPE

We focused our audit on the FDA network and Web sites in operation during the period October 21, 2013, through November 10, 2013. We did not review FDA's overall internal control structure.

METHODOLOGY

We prepared a Rules of Engagement document that outlined the general rules, logistics, and expectations for the penetration test, and FDA and OIG management signed it. We performed the following procedures:

- conducted information-gathering techniques to discover the following for FDA:
    - network address ranges,
    - host names,[9]
    - hosts exposed to the Internet,
    - applications running on exposed hosts,
    - operating system and application version information,
    - current patch levels of the hosts and applications residing on hosts,
    - structure of the applications and supporting servers, and
    - domain name server records;
- conducted vulnerability analysis techniques to discover possible methods of attack;
- attempted to exploit vulnerabilities identified in the vulnerability analysis to gain root- or administrator-level access to the targeted systems or other trusted-user account access;
- reviewed reports on security assessments performed by FDA or third-party organizations of FDA Internet-facing systems that we were not authorized to assess during our penetration test; and
- discussed our findings with FDA management.

[9] A host is any device connected to a computer network.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.