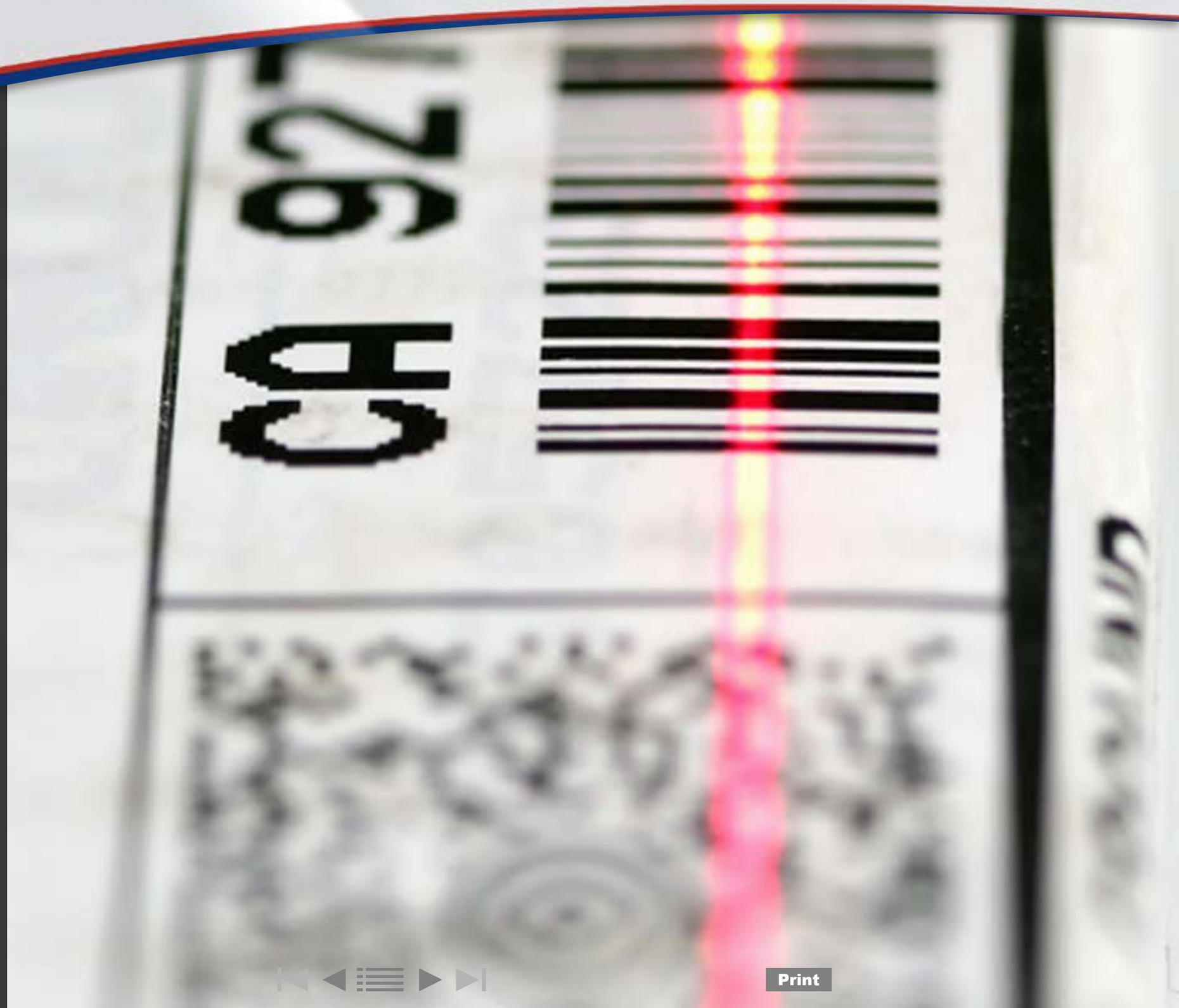
OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Parcel Readiness–Product Tracking and Reporting System Controls

Audit Report

Report Number
IT-AR-15-002

December 16, 2014



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Highlights

The Postal Service needs to improve its process for managing and securing the PTR system. Management did not safeguard eight servers that support the PTR system as required in the Postal Service security standards.

Background

The Product Tracking and Reporting (PTR) system records delivery status information for all mail with trackable services and barcodes. One of the goals of the U.S. Postal Service's Delivering Results, Innovation, Value and Efficiency Initiative 20, *Achieve 100 Percent Product Visibility*, is to provide the ability to track mailpieces and containers end-to-end through the postal network. Since PTR is vital to achieving this goal, it is important that security controls are in place to ensure the availability, integrity, and confidentiality of this application.

Our objective was to evaluate controls associated with the security, configuration, and documentation for the PTR system.

What The OIG Found

The Postal Service needs to improve its process for managing and securing the PTR system. Management did not safeguard eight servers that support the PTR system as required in the Postal Service security standards. Specifically, management did not apply critical patch updates to the operating system servers and databases. In addition, management did not properly configure the operating system, databases, and the web server to comply with security standards. Further, we determined the PTR web server contained unsupported software. Management also has not completed the disaster recovery plan for the PTR system. This occurred because management focused on other priorities such as system releases, system maintenance, and Sarbanes-Oxley Act compliance. In addition, due to a vendor software issue, management did not ensure that security configurations were reviewed on the web application server.

These security weaknesses create the potential for a malicious user to gain access to the PTR database, which could result in disclosure or modification of sensitive customer data, loss of PTR system availability, and financial liabilities. In addition, these weaknesses could allow unauthorized access to personally identifiable information, such as home addresses, phone numbers, and email addresses contained within PTR.

What The OIG Recommended

We recommended that management apply all relevant security patches to the PTR operating system servers and databases, and configure the operating system servers and databases to comply with security standards. Management should also update the PTR web server software as required, and complete the disaster recovery plan.

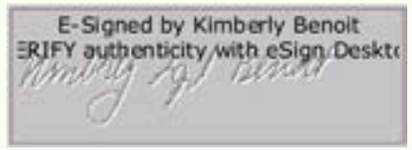
Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

December 16, 2014

MEMORANDUM FOR: JOHN T. EDGAR
VICE PRESIDENT, INFORMATION TECHNOLOGY

RICKEY T. BRANNING
ACTING MANAGER, CORPORATE INFORMATION SECURITY OFFICER



FROM: Kimberly F. Benoit
Deputy Assistant Inspector General
for Technology, Investment and Cost

SUBJECT: Audit Report – Parcel Readiness – Product Tracking and Reporting System Controls (Report Number IT-AR-15-002)

This report presents the results of our audit of Parcel Readiness – Product Tracking and Reporting System Controls (Project Number 14BR003IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Aron B. Alexander, director, Information Technology, or me at 703-248-2100.

Attachment

cc: Corporate Audit and Response Management

Table of Contents

Findings

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's Parcel Readiness – Product Tracking and Reporting (PTR) System Controls (Project Number 14BR003IT000). Our objective was to evaluate controls associated with the security, configuration, and documentation for the PTR system. See Appendix A for additional information about this audit.

PTR (formally known as Product Tracking System-II) went into production in April 2013, and provides tracking and performance data for all domestic and international package and extra services products.[1] It is the system of record[2] for all delivery status information for letter mail and parcels with trackable services and barcodes. PTR helps the Postal Service meet the goal of its Delivering Results, Innovation, Value and Efficiency (DRIVE)[3] Initiative 20, *Achieve 100 Percent Product Visibility*, by tracking mailpieces and containers end-to-end through the Postal Service network and providing business intelligence to enhance operational performance and provide customer value.

PTR system components include seven [redacted] operating system servers that contain three [redacted] databases and a PTR development web server. All eight servers support the PTR application and reside at the [redacted], Information Technology/ Computer Operations Service Center (IT/COSC). Two of the databases, a production database and a stand-alone database for data storage and expansion, are at the IT/COSC. The third is a stand-alone database at the backup and recovery site in [redacted]

Corporate Information Security provides security hardening standards[4] specifically for the [redacted] operating system and [redacted] databases. These standards support the creation of a security infrastructure and protect Postal Service electronic business applications and sensitive customer data. In addition, these standards help to ensure that system controls[5] are established to prevent vulnerabilities and systems are patched timely. When standards or system controls are not implemented in accordance with security hardening standards, systems can be at risk for accidental or intentional unauthorized use, modification, or disclosure of sensitive data.

The Computer Operations Disaster Recovery group maintains a Disaster Recovery Plan (DRP) for each application. The plan establishes the order for systematic recovery if a system is seriously damaged or destroyed. Testing must be performed on a regular basis to ensure the applications can actually be recovered.

Conclusion

The Postal Service needs to improve its process for managing and securing the PTR system. Management did not safeguard the eight servers that support the PTR system as required in the Postal Service security standards. Specifically, management did not apply critical patch updates to the operating system servers and databases. In addition, management did not properly configure the operating systems, databases, and web servers to comply with security standards. Further, we identified a PTR web server that contained unsupported software. Finally, we determined management has not completed the DRP for the PTR system.

---

1 Extra service products are items such as registered, certified, and insured mail return receipt, and Postal Service tracking and signature confirmation.
2 A system of record is a group of records from which information is retrieved by the name of an individual, or by any number, symbol, or other unique identifier assigned to that individual.
3 DRIVE is a management process the Postal Service uses to improve business strategy development and execution.
4 Standards that provide security requirements and controls for all information resources. They apply to all devices with connectivity to the Postal Service's computing infrastructure including, but not limited to, server hardware or devices operating server software, such as databases, operating systems, and servers.
5 System controls include security management, access controls, configuration management, segregation of duties, and contingency planning.

These vulnerabilities occurred because management focused on other priorities such as system releases, system maintenance, and Sarbanes-Oxley Act (SOX) compliance. In addition, due to a vendor software issue, management did not ensure that security configurations were reviewed on the web application server.

These vulnerabilities occurred because management focused on other priorities such as system releases, system maintenance, and Sarbanes-Oxley Act (SOX) compliance. In addition, due to a vendor software issue, management did not ensure that security configurations were reviewed on the web application server. These security weaknesses create the potential for a malicious user to gain access to the PTR database, which could result in disclosure or modification of sensitive customer data, loss of PTR system availability, and financial liabilities. In addition, these weaknesses could allow unauthorized access to personally identifiable information (PII), such as home addresses, phone numbers, and email addresses contained within the PTR system.

Patch Management Compliance

Patch management compliance involves reviewing and applying patches, which are small pieces of software used to correct a problem within a database or an operating system server. Using automated scanning tools[6] we scanned the PTR operating servers and databases for patch compliance during the week of June 9, 2014. We determined management did not apply some patch updates to the operating system and database servers. Specifically:

- Management did not apply the [redacted] patch to the PTR [redacted] operating system servers as required by the security standards.[7] Computer Operations[8] management notified the development team of the required solution; however, the development team's management did not apply the patch due to higher priorities related to the new PTR system price change releases and other patches. We identified four other missing patches, but they were released between quarterly patch cycles and were applied during our audit. See Appendix B for a listing of the missed patches.

- We also determined the PTR development team did not apply 12 security-related critical patch updates[9] recommended by Database Management Services[10] to the three PTR [redacted] databases. Management stated that they did not have the resources to implement and test the patch updates. As a result of our audit, management is reviewing and updating their patch management process. See Appendix C for specific details regarding the critical patch updates.

Postal Service policy[11] states that all security patches should be applied on a quarterly basis.[12] If patch updates are not applied, a malicious user could exploit and gain access to the PTR operating systems or databases, resulting in disclosure or modification of customer PII data, loss of PTR system availability, and financial liabilities.

---

6 Using specialized scanning tools such as [redacted], we scanned the operating system, the [redacted] database environment, and the non-production environment.
7 Handbook AS-805, *Information Security*, Section [redacted] Patch Management, May 2014.
8 Computer Operations in [redacted], manages the systems programming, operation, data and security for mainframe, Windows, [redacted] middleware, database, Enterprise Data Warehouse, and disaster recovery computer systems and applications.
9 [redacted] releases a critical patch update that contains security patches. Each security patch is assigned a level of criticality from one to 10 by [redacted] Administrators are required to evaluate each critical patch update to determine if the patches are relevant to the application/database.
10 Database Management Services is in the IT Service Center, [redacted].
11 *Postal Service Security Hardening Standards* [redacted] Apply All Security Patches, Revision [redacted]
12 Administrators are required to evaluate each update to determine if the patches are relevant to the application/database.

Configuration Compliance

We found that management did not properly configure the operating system, databases, and the web server to comply with security and industry standards. Specifically:We found that seven [redacted] servers did not align with Postal Service hardening standards.[13] See Appendix D for details of the [redacted] operating system settings we reviewed. [redacted] operating system administrators configured the settings according to the hardening standards; however, the PTR application and middleware[14] owners altered the server settings to support further business functionality, in accordance with the [redacted] Configuration Baseline which differed from the hardening standards.[15] This occurred because the documentation contained in the Postal Service's Hardening Standards and the [redacted] Configuration Baseline does not have the same requirements for these settings. As a result of our audit, management is updating the hardening standards.

- We identified five security settings that did not comply with Postal Service's hardening standards[16] for the three [redacted] databases supporting PTR. See Appendix E for details about the specific configuration settings we identified. [redacted] database hardening standards were updated in [redacted], requiring Database Services[17] to change the default settings we identified. Management indicated these updates were not completed when we finalized our testing in June because of priorities related to day-to-day operation support for tasks such as SOX and Payment Card Industry (PCI) compliance.

- We determined that [redacted] databases were susceptible to the [redacted], which would allow an attacker to gain access to a database. Although [redacted] has released a solution[19] for this vulnerability, management did not have an opportunity to test and implement the solution. Higher priorities such as the day-to-day operation support for tasks such as SOX and PCI compliance took precedence over addressing this vulnerability.

- We identified three security vulnerabilities on the PTR development web server[20] that could allow for potential unauthorized access to the PTR database. See Appendix F for details on the three vulnerabilities. Policy[21] requires that all web servers, regardless of location, use approved hardware and software with standard configurations to reduce the likelihood of loss or compromise due to exploitation of configuration vulnerabilities. Management said a vendor software issue allowed for the [redacted] to occur. The remaining two vulnerabilities were caused by a lack of a code review on the web development server.

Not adhering to Postal Service security standards could result in data corruption or loss, unauthorized access by hackers, inappropriate changes to computer programs, physical damage to servers, or installation of malware. These security weaknesses create the potential for unauthorized access to PII contained within the PTR system. Therefore, we estimated data at risk of about $137 million for 161 million records containing sensitive information that are processed daily through the PTR system.

---

13 *Postal Service Server Hardening Standards for* [redacted] *Operating Systems*, Sections [redacted]
14 A program that exists between a "network" and an "application" and carries out such tasks as authentication.
15 Postal Service [redacted] Configuration Baseline, [redacted], provides standards of how the [redacted] operating system should be created using the [redacted] building.
16 *Postal Service Security Hardening Standards* [redacted].
17 [redacted] database administrations are in [redacted] and are responsible for applying approved patches and modifications in accordance with Postal Service policies and procedures.
[redacted]
19 [redacted] released the [redacted]
20 Since the [redacted] scanning tool could potentially corrupt the PTR data, we used non-production web servers that mirrored the production web servers to provide assurance that our vulnerability scans would not affect the production environment.
21 Handbook AS-805, Section [redacted] Using Web Servers.
[redacted]

Disaster Recovery Plan

Management does not have a complete DRP[23] specific to PTR as required by policy.[24] Management is working on the DRP, with an estimated completion date of February 2015, and has stated the final version will include the following two availability tiers:[25]

- Tier 1 functionalities include the Track and Confirm[26] function of PTR.
- Tier 2 functionalities ensure the availability of scans, manifest ingestion, customer extracts, achieved scan lookups, and operational reporting.

At the time of our audit, the PTR system development team had completed and tested the functionalities of the Tier 1 portion of the DRP; however, management has not developed the Tier 2 portions, which will address all functionalities of PTR. The DRP was not completed because management was focused on other priorities such as system releases, system maintenance, and other daily operations. During our audit, management continued to work through the DRP solutions with the service providers. Without a DRP, management cannot ensure the availability of PTR in the event of system disruption. In addition, management may not be able to provide accurate tracking information to its customers regarding the delivery status of mail and parcels in the event of system disruption.

Other Matter

The U.S. Postal Service Office of Inspector General (OIG) found an internal-facing development web server running software that is no longer supported by the vendor. Specifically, the PTR development[27] web server is running [redacted] which is using a version of [redacted] the vendor stopped supporting as of [redacted]. [redacted] is included with the bundle for [redacted] and cannot be updated separately. The option to update [redacted] outside of [redacted] is not technically feasible. Management plans to work with the vendor to evaluate possible software updates and address this issue. Since this is a development web server that is not externally accessible, we do not plan to issue a recommendation at this time.

23 The Computer Operations Disaster Recovery group uses the DRP to establish the order for systematic recovery if a system or facility is seriously damaged or destroyed.
24 Handbook AS-805, Section 12-5, Disaster Recovery Plan Requirements.
25 The [redacted] group uses a tiered approach to define the availability requirements for the PTR System. The approach allows for the investment and risk associated with ultra high-availability deployment to be targeted towards the right set of business and system capabilities.
26 The Track and Confirm Web Tool lets customers determine the delivery status of their Priority Mail, Express Mail, and Package Services (Standard Post, Bound Printed Matter, Library Mail, and Media Mail) packages with Delivery Confirmation.
27 Management uses a non-production web server that mirrored the production web servers for testing, evaluation, and to configure scripts for the PTR System.
28 The Postal Service uses [redacted] to start-up, shut down, and configure scripts.
29 Software used to run a web server.

Recommendations

We recommend management address the vulnerabilities identified in this report, align the [redacted] Configuration Baseline Standards with the Hardening Standards for [redacted] Operating Systems, and complete their Tier 2 Disaster Recovery Plan.

We recommend the vice president, Information Technology, direct the manager, Computer Operations, to:

1. Apply the [redacted] critical patch updates we identified to the Product Tracking and Reporting system databases. In addition, configure the operating system servers and databases in accordance with Postal Service hardening standards.

2. Test and implement the [redacted] to resolve the [redacted] impacting the Product Tracking and Reporting database.

We recommend the vice president, Information Technology, coordinate with the acting manager, Corporate Information Security Officer, to:

3. Align the Product Tracking and Reporting system [redacted] Configuration Baseline Standards with the Postal Service Sever Hardening Standards for [redacted] Operating Systems.

We recommend the vice president, Information Technology, direct the manager, Solutions Development and Support, to:

4. Update the [redacted] patch to the current version for the Product Tracking and Reporting system Websphere environment.

5. Perform a review of the web server security settings for the Product Tracking and Reporting (PTR) system development web server and fix any identified vulnerabilities. In addition, identify a solution with the vendor to remove the [redacted] vulnerability from the PTR system development web server.

6. Complete the Product and Tracking Reporting system Tier 2 Disaster Recovery Plan.

Management's Comments

Management partially agreed with recommendation 1 and agreed with the findings and recommendations for 2, 4, 5, and 6. Management disagreed with recommendation 3.

Regarding recommendation 1, management will coordinate with the [redacted] to apply the [redacted] critical patch updates to the system databases. In addition, management agreed to configure the PTR databases where possible and request a Risk Acceptance Letter for those hardening standards that PTR cannot comply with. Management's target implementation date is March 31, 2015.

Regarding recommendation 2, management will deploy the [redacted] to address the [redacted] to the PTR database. Management's target implementation date is March 31, 2015.

Regarding recommendation 3, management stated there is no deviation in the PTR[redacted] Configuration Baseline Standards from the current[redacted] Configuration Baseline Standards or Postal Service Hardening Standards for [redacted] Operating Systems.

Regarding recommendation 4, management stated it applied the [redacted] Patch for the Websphere environment on October 26, 2014. Management requested that recommendation 4 be closed out with the issuance of the final audit report.

Regarding recommendation 5, management will perform a review of the web server security settings for the PTR development web server and fix any identified vulnerabilities by September 30, 2015. Management deems that the [redacted] is from related software and not publicly accessible. Therefore management states corrective action is a low priority and will be addressed when the product is upgraded prior to the End-of-Life date of [redacted].

Regarding recommendation 6, the PTR Disaster Recovery Plan is part of the work outlined in the PTR Fiscal Year 2015 IT Expansion Plan, which is contingent upon funding approval. Management's target implementation date is Septemer 30, 2015.

See Appendix G for management's comments, in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1, 2, and 4 through 6, and the corrective actions should resolve the issues identified in the report. The OIG considers management's comments to recommendation 3 to be non-responsive.

Regarding management's response to recommendation 3, the OIG is reporting a difference between the Postal Service Hardening Standards for [redacted] Operating Systems and the PTR system [redacted] Configuration Baseline Standards. The hardening standards have multiple options to comply with the standard, whereas the baseline configuration is specific and is limited to one option. From a security perspective, management should consider implementing the most restrictive option until the two documents are reconciled. The OIG used the hardening standards to perform its testing and identified the vulnerabilities reported. Therefore, the Postal Service should review and align these standards accordingly.

Regarding management response to recommendation 5, action in response to the recommendation should remain a priority and be addressed as soon as the product upgrade is available to prevent[redacted]

The OIG considers recommendations 1, 4, and 6 significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

Click on the appendix title to the right to navigate to the section content.

Appendix A: Additional Information

Background

In 2011, the Postal Service approved the Product Tracking Re-Engineering Decision Analysis Report for $89.3 million in capital investment funding to integrate and consolidate several core functions of the existing product tracking system. Management made this investment to enable the capacity to handle future growth in volume, barcodes, scan events, and business data; and provide near real time data processing, posting, and provisioning.

PTR uses the [redacted] operating system running on seven servers and a development web server for testing and making changes to PTR. In addition, PTR is comprised of three databases: one production database; one stand-alone database in IT/COSC in [redacted] that is used for data storage and expansion as needed; and an additional stand-alone database at the backup and recovery site in [redacted] Database Services[30] is responsible for setting up PTR databases and data backup and recovery. Management conducts full system backups at least once a week, incremental backups every other day, and archives log backups daily. In addition, the Computer Operations[31] group conducts all the disaster recovery testing and evaluation for all Postal Service applications. Policy also requires that each application have a separate DRP stored in the Technology Solutions Life Cycle IT Artifact Library. According to policy, the development organization and the executive sponsor must certify any DRP testing.

The [redacted] group[32] is responsible for overall PTR project management and system development. Along with the business executive, this group works with onsite contractors to manage the system. In addition, this group measures and monitors PTR performance on a regular basis. The Solutions Center group sends performance metrics to management for their review on a daily basis. This information includes metrics on system availability, tracking and upload response times, transmission, and other information.

Objective, Scope, and Methodology

Our objective was to evaluate controls associated with the security, configuration, and documentation for the PTR system. During this audit, we reviewed the PTR system production and development environments related to security, configuration, and documentation. Our audit did not include evaluating quality and integrity of data within the PTR system. Specifically, we conducted a vulnerability assessment of PTR servers located at the IT/COSC in [redacted]. In addition, we reviewed hardening standards and best practices, and scanned the non-production computing environment identified by IP addresses. Using specialized tools such as [redacted] we scanned the operating system servers, the [redacted] database environment, and the development web server. We conducted this vulnerability assessment to determine if the PTR computing environment is configured, patched, and managed according to Postal Service hardening standards and industry best practices. We analyzed the data, identified and summarized any security issues associated with PTR, and discussed these results

30 Database Services is in the [redacted] IT Service Center.
31 Computer Operations in [redacted], and [redacted] manages the systems programming, operation, data and security for mainframe, Windows, UNIX, middleware, database, Enterprise Data Warehouse, and disaster recovery computer systems and applications.
32 The [redacted] group is under the IT Solutions Development and Support team. This group is responsible for managing the development, maintenance, and enhancement of business systems; overseeing the transition of systems developed by business partners to an internal supported environment, and supporting ongoing changes and new functionality.
33 [redacted] is a network-based, discovery and vulnerability scanner that discovers database applications within the infrastructure and assesses their security strength.
34 [redacted] a vulnerability and configuration assessment product that features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis.
35 [redacted] is an automated and configurable web application security and penetration-testing tool that mimics real-world hacking techniques and attacks, enabling the user to analyze complex web applications and services for security vulnerabilities.

with Computer Operations, [redacted] ASC/IT management, and the [redacted] group management. Finally, we met with management to determine the status of outstanding security documentation associated with the PTR Certification and Accreditation process, obtained documentation regarding a DRP, and reviewed current documentation regarding PTR system performance and metrics.

We conducted this performance audit from March through December 2014, in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on November 6, 2014, and included their comments where appropriate.

We assessed the reliability of operating system and database configuration data by performing electronic testing of the hosts, reviewing resultant data for false positives and other anomalies, and interviewing agency management knowledgeable about the data. We determined the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact (in millions)
Topeka, KS, Material Distribution Center – Information Technology Logical Access Controls	IT-AR-14-007	7/11/2014	None
Report Results: The Material Distribution Center (MDC) did not adequately safeguard the 14 servers that support the check printing and inventory management applications, thereby jeopardizing the security of their data. Specifically, management did not update the operating systems on any of the 14 servers or configure three database servers in accordance with security standards. In addition, the MDC did not use [redacted] software on two servers or adequately protect [redacted] server from unauthorized use. We made three recommendations related to properly configuring databases, verifying that the latest approved [redacted] software is enabled on operating systems, and developing a process to ensure security configurations are reviewed on all web servers. Management agreed with all the findings and recommendations in the report.			

Appendix B: [redacted] Operating System Patching

Table 1 summarizes the five high-risk or critical-risk patch updates the Postal Service OIG automated scanning tools determined were missing from one or more of the PTR[redacted] servers. The patch publication dates for the required high-risk patches range from March through May 2014.

Table 1. [redacted] Operating System Patching Vulnerabilities

VULNERABILITY CHECKS AND NON-COMPLIANCE ISSUE DESCRIPTION	[redacted] SERVERS							TOTAL	RISK FACTOR
PATCH NAME	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]		
[redacted]		1		1				2	High
[redacted]	1	1	1	1	1	1	1	7	Critical
[redacted]	1	1	1	1	1	1	1	7	High
[redacted]	1	1	1	1	1		1	6	Critical
[redacted]	1	1	1	1	1	1	1	7	High
Total	4	5	4	5	4	3	4	29	

36 This patch was released by [redacted]
37 This patch was released by [redacted]
38 This patch was released by [redacted]
39 This patch was released by [redacted]

Appendix C: [redacted] Patch Management

Table 2 summarizes the 12 critical patch updates that were missing from one or more of the three PTR database servers. The implementation date for the required high-risk patches range from January 2011 through October 2013. Table 2 summarizes the 12 critical patch updates by date.

Table 2. [redacted] Critical Patch Updates

Number	Missing High-Risk Updates	Risk Factor
1	Critical Patch Update - [redacted]	High
2	Critical Patch Update - [redacted]	High
3	Critical Patch Update - [redacted]	High
4	Critical Patch Update - [redacted]	High
5	Critical Patch Update - [redacted]	High
6	Critical Patch Update - [redacted]	High
7	Critical Patch Update - [redacted]	High
8	Critical Patch Update - [redacted]	High
9	Critical Patch Update - [redacted]	High
10	Critical Patch Update - [redacted]	High
11	Critical Patch Update - [redacted]	High
12	Critical Patch Update - [redacted]	High

Appendix D: [redacted] Operating System Configuration

Table 3 summarizes the settings we reviewed to determine if the [redacted] operating system was configured in accordance with Postal Service hardening standards. The "✓" in the table identifies the servers that were compliant with hardening standards and the "x" identifies servers that were not compliant with the hardening standards. For example, our scans identified the [redacted] was enabled since PTR database administrators added [redacted] after the [redacted] baseline configuration was created.

Table 3. [redacted] Operating System Configuration

Category	Compliance Check	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]								
	[redacted]	✓	✓	✓	✓	✓	✓	✓
[redacted]								
	[redacted]	✓	✓	✓	✓	✓	✓	✓
[redacted]								
	[redacted]	✓	✓	✓	✓	✓	✓	✓
[redacted]								
	[redacted]	✓	✓	✓	✓	✓	✓	✓
	[redacted]	✓	✓	✓	✓	✓	✓	✓
	[redacted]	✓	✓	✓	✓	✓	✓	✓
	[redacted]	✓	✓	✓	✓	✓	✓	✓
[redacted]								
	[redacted]	✓	☒	✓	✓	☒	✓	☒
	[redacted]	✓	✓	✓	✓	✓	✓	✓
	[redacted]	✓	✓	✓	✓	✓	✓	✓
	[redacted]	✓	✓	✓	✓	☒	☒	☒
[redacted]								
	[redacted]	✓	✓	✓	✓	✓	✓	✓
	[redacted]	✓	✓	✓	✓	✓	✓	✓
	[redacted]	✓	✓	✓	✓	✓	✓	✓
[redacted]								
	[redacted]	✓	✓	✓	✓	✓	✓	✓
	[redacted]	✓	✓	✓	✓	✓	✓	✓
	[redacted]	✓	✓	✓	✓	✓	✓	✓

Appendix E: [redacted] Database Configuration

Table 4 summarizes the [redacted] database security settings we reviewed and the associated categories for all three PTR database servers. The OIG used the [redacted] scanning tool to check the database configurations against Postal Service Security [redacted] Database hardening standards. We identified five vulnerability checks that did not comply with the hardening standards for all three PTR databases.

Table 4. Vulnerability Checks and Non-Compliance Issues

Category	Vulnerability	Database Servers		
		[redacted]	[redacted]	[redacted]
[redacted]				
	[redacted]	x	x	x
	[redacted]	x	x	x
[redacted]				
	[redacted]	x	x	x
	[redacted]	x	x	x
[redacted]				
	[redacted]	x	x	x
Totals		**5**	**5**	**5**

[redacted]

Appendix F:
Web Server Vulnerabilities

Appendix F summarizes the three vulnerabilities found on the development web server. The OIG used the [redacted] scanning tool to check the development web server for the following vulnerabilities:

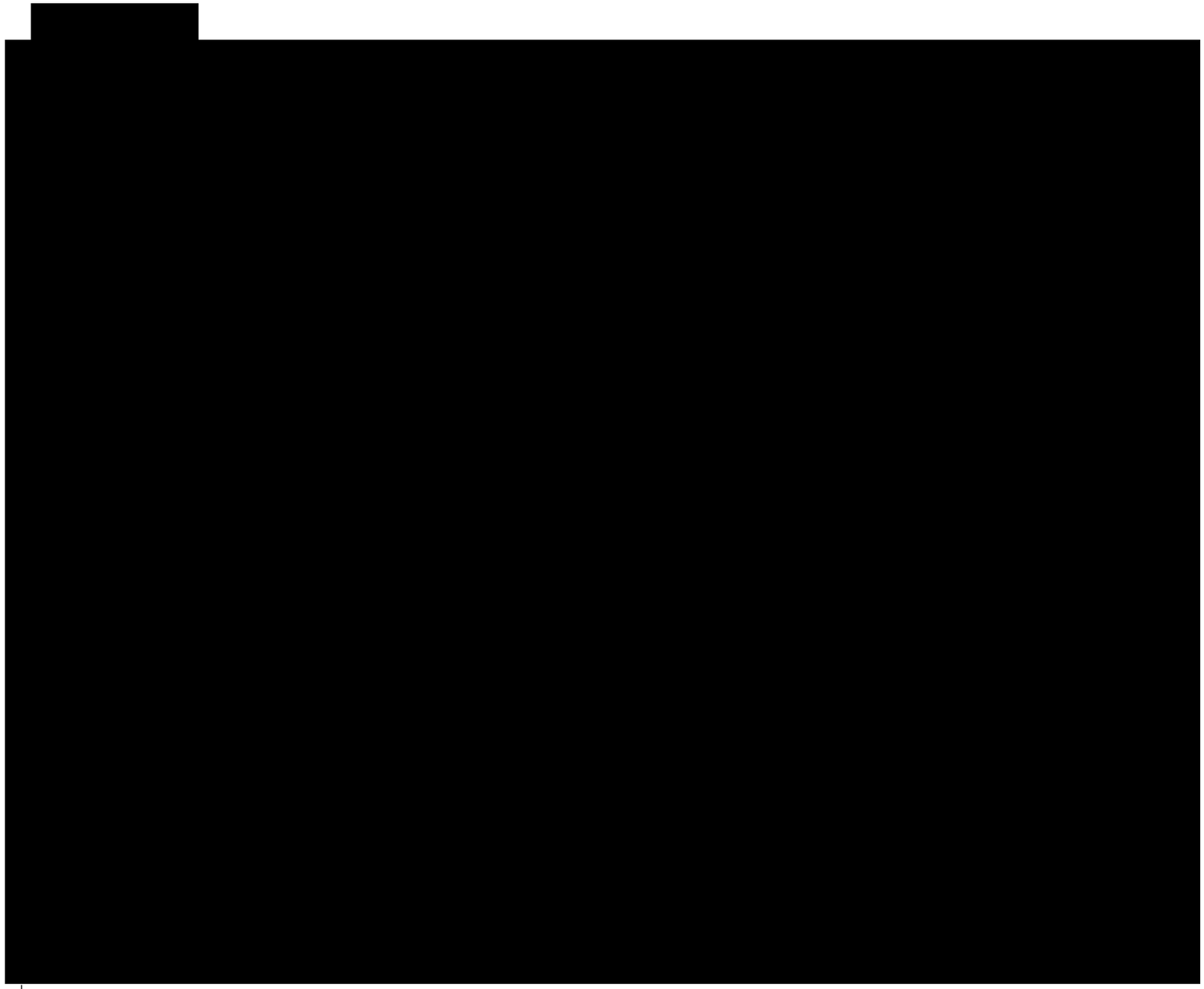
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

46 A worldwide organization focused on improving the security of software.

[redacted]



[redacted]

[redacted]

[redacted]

[redacted]

48 A global management consulting firm focused on information security.

Appendix G: Management's Comments

JOHN T. EDGAR
VICE PRESIDENT
INFORMATION TECHNOLOGY

UNITED STATES POSTAL SERVICE

November 21st, 2014

LORI LAU DILLARD
DIRECTOR, AUDIT OPERATIONS (A)

SUBJECT: Response to Draft Report: Parcel Readiness – Product Tracking & Reporting System Assessment (IT-AR-15-DRAFT)

Recommendation [1]:
Apply the [redacted]critical patch updates we identified to the Product Tracking and Reporting system databases. In addition, configure the operating system servers and databases in accordance with Postal Service hardening standards.

Management Response:
Management partially agrees with the recommendation. [redacted]will coordinate to apply the [redacted]critical patch updates to the system databases. We partially agree with the recommendation to configure operating system databases. We will configure the PTR databases where possible and request a Risk Acceptance Letter for those hardening standards that PTR cannot comply with.

Target Implementation Date:
March 31, 2015

Responsible Official:
Manager, [redacted]Information Technology

Recommendation [2]:
Test and implement the [redacted]solution to resolve the [redacted]impacting the Product Tracking and Reporting database.

Management Response:
Management agrees with the recommendation. The [redacted]will be deployed to address the [redacted]to the PTR database.

Target Implementation Date:
March 31, 2015

Responsible Official:
Manager, Computer Operations, Information Technology

Recommendation [3]:
Align the Product Tracking and Reporting system [redacted]Configuration Baseline Standards with the Postal Service Sever Hardening Standards for [redacted]Operating Systems.

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-2100
202-268-3977
FAX: 202-268-4492
JOHN.T.EDGAR@USPS.GOV
WWW.USPS.COM

Management Response:
Management disagrees with the recommendation. There is no deviation in the Product Tracking and Reporting system [redacted] Configuration Baseline Standards from the current [redacted] Configuration Baseline Standards or Postal Service Hardening Standards for [redacted] operating systems.

Responsible Official:
Manager, Computer Operations, Information Technology

Recommendation [4]:
Update the [redacted] patch to the current version for the Product Tracking and Reporting system Websphere environment.

Management Response:
Management agrees with the recommendation. The [redacted] Patch for the Websphere environment was applied on [redacted] We request that Recommendation 4 be closed out with the issuance of the final audit report.

Responsible Official:
Manager, Solutions Development & Support, Information Technology

Recommendation [5]:
Perform a review of the web server security settings for the Product Tracking and Reporting system development web server and fix any identified vulnerabilities. In addition, identify a solution with the vendor to remove the [redacted] vulnerability from the Product Tracking and Reporting system development web server.

Management Response:
Management agrees with the recommendation. Management will perform a review of the web server security settings for the Product Tracking and Reporting system development web server and fix any identified vulnerabilities. Management deems that the [redacted] vulnerability is low priority, due to the following:

1) The [redacted] vulnerability is from the [redacted] Software and not from the Product Tracking and Reporting System.
2) The site is not available from the vIP and is only reachable for persons with approved firewall access to the Web/App Tier server.

The vulnerability will be addressed when the product is upgraded prior to the End-of-Life date of [redacted]

Target Implementation Date:
September 30, 2015

Responsible Official:
Manager, Solutions Development & Support, Information Technology

475 L'Enfant Plaza SW
Washington DC 20260-2100
202-268-3977
Fax: 202-268-4492
JOHN.T.EDGAR@USPS.GOV
WWW.USPS.COM

Recommendation [6]:
Complete the Product and Tracking Reporting system Tier 2 Disaster Recovery Plan.

Management Response:
Management agrees with the recommendation. The PTR Disaster Recovery Plan is part of the work outlined in the PTR FY15 IT Expansion Plan. Implementation of the PTR FY15 IT Expansion Plan will be contingent upon funding approval.

Target Implementation Date:
September 30, 2015

Responsible Official:
Manager, Solutions Development & Support, Information Technology

FOIA Statement:
This report contains information which management believes may contain proprietary or other business information that may be exempt from disclosure under the Freedom of Information Act (FOIA).

The following sections should be redacted from the final audit report. These sections contain information that could be used by a hacker to cause harm to the USPS network and associated systems:

[redacted]

John T. Edgar
Vice President, Information Technology

cc: *Sally K. Haring, Manager, Corporate Audit Response Management*

475 L'Enfant Plaza SW
Washington DC 20260-2109
202-268-3977
Fax: 202-268-4492
JOHN.T.EDGAR@USPS.GOV
WWW.USPS.COM

OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms, follow us on social networks, or call our Hotline at 1-888-877-7644 to report fraud, waste or abuse. Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100