

OFFICE OF INSPECTOR GENERAL UNITED STATES POSTAL SERVICE

Capital District Vulnerability Assessment

Audit Report

Report Number IT-AR-15-001

December 12, 2014





OFFICE OF INSPECTOR GENERAL UNITED STATES POSTAL SERVICE

Highlights

These vulnerabilities expose the infrastructure to unauthorized remote access by potential attackers who may discover network weaknesses, retrieve information, corrupt data, and reconfigure settings.

Background

The U.S. Postal Service Office of Inspector General's Information Technology Security Risk Model identified the Capital District as being among the five most at-risk districts for multiple quarters during fiscal years (FY) 2013 and 2014. Security events during those periods included instances of malicious software which can affect the confidentiality, integrity, and availability of sensitive data and potentially compromise critical mail processing applications.

During FY 2013, the Capital District processed about 2 billion mailpieces and generated about \$470.9 million in revenue. The district had about 6,600 employees working in 260 facilities during that time.

Our objective was to review system security controls in the Capital District to determine whether proper security exists to protect U.S. Postal Service infrastructure and data.

What The OIG Found

Security controls in the Capital District did not adequately protect Postal Service infrastructure and data from unauthorized access or corruption. Of the 1,254 systems active on the network, we tested 33 and detected a combined total of 417 vulnerabilities, such as missing security updates or system configuration deficiencies. Of the 417 vulnerabilities, 79 were considered critical and high-risk for which patches were available for at least 1 year. We further identified four active

and two shared user accounts. These vulnerabilities expose the infrastructure to unauthorized remote access by potential attackers who may discover network weaknesses, retrieve information, corrupt data, and reconfigure settings.

The Capital District also permits access to devices using unsecure communications, which further threatens network security. Finally, we identified weaknesses in asset management and accountability that could allow an unauthorized device to remain on the network undetected.

These vulnerabilities occurred because administrators improperly configured systems, did not install the latest patch updates, and did not employ uniform processes to manage information system assets.

What The OIG Recommended

We recommended management evaluate, test, and install critical patches and correct configuration settings on the identified databases and operating systems. We also recommended management disallow software that permits unsecure communications, discontinue the use of shared user accounts, and uniformly manage assets. Additionally, we recommended management remove the from databases.

Capital District Vulnerability Assessment

Configuration vulnerabilities can allow unauthorized users to gain access to data, services, and sensitive information.

The U.S. Postal Service OIG's Information Technology Security Risk Model identified the Capital District as being among the five most at-risk districts for multiple quarters during FY 2013 and 2014.

Security controls in the Capital District did not adequately protect Postal Service infrastructure and data from unauthorized access or corruption.



Transmittal Letter

United States Postal	Service
December 12, 2014	
MEMORANDUM FOR:	JAMES P. COCHRANE CHIEF INFORMATION OFFICER AND EXECUTIVE VICE PRESIDENT
	MICHAEL J. AMATO VICE PRESIDENT, ENGINEERING SYSTEMS
	JOHN T. EDGAR VICE PRESIDENT, INFORMATION TECHNOLOGY
	KRISTIN A. SEAVER VICE PRESIDENT AREA OPERATIONS, CAPITAL METRO AREA
FROM:	E-Signed by Kimberly Benoit ERIFY authenticity with eSign Deskto Mimberly F. Benoit Deputy Assistant Inspector General
	for Technology, Investment and Cost
SUBJECT:	Audit Report – Capital District Vulnerability Assessment (Report Number IT-AR-15-001)
This report presents the r Vulnerability Assessment	esults of our audit of the U.S. Postal Service's Capital Dis (Project Number 13WG012IT000).
We appreciate the coope questions or need additio Information Technology, c	ration and courtesies provided by your staff. If you have a nal information, please contact Aron Alexander, director, or me at 703-248-2100.
Attachment	
cc: Corporate Audit and	Response Management

Table of Contents

Cover	
Highlights	1
Background	1
What The OIG Found	1
What The OIG Recommended	1
Transmittal Letter	3
Findings	5
Introduction	5
Conclusion	5
Configuration Management	6
Patch Management	7
Remote Access	9
Asset Management and Accountability	10
Recommendations	11
Management's Comments	12
Evaluation of Management's Comments	13
Appendices	14
Appendix A: Additional Information	15
Background	15
Objective, Scope, and Methodology	15
Prior Audit Coverage	16
Appendix B: Configuration Management Vulnerabilities	17
Appendix C: Patch Management Vulnerabilities	19
Appendix D: Management's Comments	20
Contact Information	27

Findings

We found 33 systems with an aggregate of 417 critical and high-risk vulnerabilities.

Introduction

This report presents the results of our self-initiated audit of the U.S. Postal Service's Capital District Vulnerability Assessment (Project Number 13WG012IT000). Our objective was to review system security controls in the Capital District to determine whether proper security exists to protect Postal Service infrastructure and data. See Appendix A for additional information about this audit.

The U.S. Postal Service Office of Inspector General (OIG) prepares a quarterly Information Technology (IT) Security Risk Model to provide stakeholders with an overview of security in their respective areas of responsibility. The model is an evaluation of data retrieved from the **security events**¹ identifying instances of security events² on information systems at the district level. These security events could expose Postal Service information, data, programs, and equipment to multiple exploits that could disrupt the operation of critical mail processing equipment (MPE).

The combined IT Security Risk Model, which included the fiscal year (FY) 2012, Quarter (Q) 4 and FY 2013 Q1 through Q3, presented the Capital District as the most at-risk district with regard to the number of security events. Trend data from additional quarters (FY 2013, Q4 and FY 2014, Q1) show the Capital District remained among the five highest risk districts.

The Capital District processed about 2 billion pieces of mail and generated about \$470.9 million in revenue during FY 2013. The Capital District had about 6,600 employees in 260 facilities during that time.

Conclusion

1 2

7

8 9

Security controls surrounding the Capital District did not adequately protect Postal Service infrastructure and data against potential unauthorized access or corruption. During enumeration,³ we discovered 1,254 Internet Protocol (IP) addresses representing active systems on the network in the Capital District. We evaluated 33 of the systems for patch vulnerabilities. Of these 33 systems, 29 were also evaluated for configuration management.⁴

Using network security analyzers,⁵ we scanned the systems and identified an aggregate of 417 critical and high-risk vulnerabilities



- 5 Tools used to scan the network for security vulnerabilities. We used the following tools for this audit:
- 6 The Postal Service uses to simplify, standardize, and efficiently manage its IT environment. information systems are centrally managed and supported and only approved standardized software packages are authorized.
 - systems are information systems that communicate with MPE, such as:

The obtains security event data from antivirus solutions residing on computers at Postal Service district facilities. The data is used to prepare the risk models. security events include adware, spyware, Trojans, viruses, and worms.

³ The method used to discover systems on a network.

⁴ We selected 35 systems for review based on our enumeration scan results and the IT Security Risk Model. Two systems were not scanned for patch vulnerabilities because management could not identify the administrator or manager to grant access. The remaining 33 systems were tested with at least one of the security analyzers. Scan results for configuration compliance were retrieved for only 29 of the systems because management would have had to alter system registry configurations in order to provide us necessary access to complete the full scans.

These vulnerabilities occurred because administrators did not install the latest patch updates, did not employ a uniform process for managing information system assets, and improperly configured **accurred**, and **accurred**. The vulnerabilities detected place the data, programs, and equipment used in the Capital District to process the mail at risk of discovery, alteration, and corruption. Additionally, they could potentially lead to disruption of mail processing.

Configuration Management

We identified configuration vulnerabilities in 26 of the 29 and and and Linux and Windows systems we scanned. These vulnerabilities included areas of non-compliance related to operating systems, intrusion protection, accounts, passwords, and logging. Tables 1 and 2 summarize the results by compliance areas. See Appendix B for compliance detail.

Table 1. Linux Compliance

Linux Systems Scanned		3
Compliance Area	Compliant	Non-Compliant
	0	3
	0	3
	0	3
	0	3
Source: OIG and scanning tool results.		

Table 2. Windows Compliance

Windows Systems Scanned	t i	11		13		2
Compliance Area	Compliant	Non-Compliant	Compliant	Non-Compliant	Compliant	Non-Compliant
	11	0	5	8	0	2
	11	0	4	9	0	2
	3	8	0	13	0	2
Source: OIG and sc	anning tool results.					

In addition, we identified databases on two Biohazard Detection Systems (BDS) that contained . Further, three district information systems staff shared an account and password to administer the systems.

These vulnerabilities occurred in the **systems** because management uses automated procedures during the logon process that do not configure the correct audit logging settings. Management stated they are working to convert from the logon process to a group policy object¹⁰ that will contain the proper settings with a target completion date of October 1, 2015.

The **configuration** vulnerabilities occurred because the systems were duplicated from preset images that contained inappropriate settings. Management is working on a solution that will update groups of systems to consistently comply with policy. Management also stated the outdated systems would not run effectively with the software, and

In addition, contractors left the **second second** in the BDS **second** databases, although the accounts were not part of the requirements. After becoming aware of this vulnerability, management directed the contractor to resolve it.

For the systems, the district Information Systems manager stated the sector were in place when his temporary assignment began, and he was unaware of the configuration vulnerabilities.

Configuration vulnerabilities can allow unauthorized users to gain access to data, services, and sensitive information. Unauthorized user access could result in loss of critical data, services, and user accountability, which could also impact the operation of critical MPE. The absence of logs prevents the capture of historical information needed to investigate events related to failed logon attempts, unauthorized configuration changes, and other system related events.

Patch Management

Administrators did not install the latest patch updates on 11 **1**, 20**1**, 20**1**, and two **1**, and two **1**, systems. Specifically, we identified an aggregate of 417 critical and high-risk vulnerabilities on the systems we reviewed. We identified 241 patch updates that, if correctly applied, would resolve these vulnerabilities.

¹⁰ An infrastructure that allows administrators to implement specific configurations for users and computers.

Table 3 summarizes the critical and high-risk vulnerabilities for which some missing patches¹¹ were available for more than 90 days. The oldest missing patch dated back to 2004.

Table 3. Missing Linux and Windows Patch Updates

Critical and high-risk vulnerabilities were found to have missing patches available for more than 90 days.

Organization	Critical and High Risk Patch Vulnerabilities	Number of Missing Patch Updates	Number of Patch Updates Available for More Than 90 Days
	106	80	54 ¹²
	247	131	50 ¹³
	64	30	4 ¹⁴
Totals ¹⁵	417	241	108
Source: OIG and	scanning tool results.		

See Appendix C for detailed scan results.

, with no critical pat	tch updates. Further, two	databases on the BDS systems were

exposed to 184 high-risk vulnerabilities for which 22 patches were missing but available for more than 90 days, with some available since 2011.

- 11 Some vulnerabilities may exist in multiple system types.
- 12 patch updates were available since 2006.
- 13 patch updates were available since 2004.
- 14 patch updates were available since 2004.
- 15 Some patch updates will resolve multiple vulnerabilities.
- 16 The continuously collects data from all MPE in a facility allowing managers to balance equipment and staffing to workloads improving productivity.

For systems, management stated the vulnerabilities occurred because some patches had not been approved for deployment,¹⁷ and some missing patches were an oversight due to the unsupported Windows XP operating systems. During our audit, IT management scanned the **systems** and recommended re-imaging of the 10 workstations and patch updates for the server. The workstations were deactivated in Active Directory (AD)¹⁸ until they are replaced or re-imaged.

These vulnerabilities occurred for the systems because database administrators believed the systems release included the latest patches available. For the systems, the District Information Systems manager stated the were in place when his temporary assignment began, and he did not know he was responsible for patching

these systems.

Systems without up to date patches prevent the resolution of known vulnerabilities and leave the Postal Service at risk of potential unauthorized access or data corruption that could lead to unavailable resources or disruption of mail processing operations.

Remote Access

Management allowed remote access to network devices¹⁹ using unsecure communications that weaken network security. For example:

Three systems were configured to allow a user to remotely connect to a resource using the service.
In addition, two firewalls were configured to allow
²⁰ traffic to pass from one network to another network.

Two systems equipped with sectors were inappropriately connected to the network, and were not documented in the Asset Inventory Management System (AIMS)²¹ or AD. These sectors allow outsiders to perform unauthorized scans and exploit security vulnerabilities.

Engineering management stated they occasionally need service for remote administration of network devices.

Management stated the vulnerabilities occurred because management was not aware of their responsibility for securing the systems. During our audit, management disconnected the systems from the network and disconnected the system.

Remote access configuration vulnerabilities may allow unauthorized users to bypass access controls, and could allow attackers to gain network access to retrieve information, corrupt data, install malware, and change configuration settings. An unauthenticated attacker could remotely execute code,²² cause a denial of service,²³ gain unauthorized access to files or systems, modify critical data, or delete backup information.

20 allows a user to remotely connect to a resource using the protocol but transmits

Management allowed remote access to network devices using unsecure communications that weaken network security.

¹⁷ As of July 8, 2014.

¹⁸ AD enables centralized, secure management of an entire network, which might span a building, a city, or multiple locations throughout the world.

¹⁹ Network devices are workstations, servers, databases, routers, switches, and other systems communicating on the network.

²¹ AIMS automates the collection of most IT assets like workstations, laptops, and servers. It allows users to interactively query the asset database using a variety of search results to review, analyze, and maintain Postal Service networked and non-networked asset inventory.

²² Remote code execution is the ability an attacker has to access someone else's computing device and make changes, no matter where the device is geographically located. An attacker can use vulnerabilities to execute malicious code and take complete control of an affected system with the privileges of the user running the application.

²³ Loss of network or computer services due to resource limitations or resource exhaustion, performance problems, or hardware/software failures.

Asset Management and Accountability

Management did not adequately protect the network infrastructure with a uniform asset management process. During our audit, we asked the Postal Service IT and Engineering audit response coordinators (ARCs) for the names of system administrators and managers who could give us appropriate access to network devices. We determined:

- Management could not always correctly identify the administrators and managers assigned to network devices. In some instances, the IT ARC contacted multiple employees before identifying the correct administrator. In addition, the Engineering ARC provided three primary contacts from the IP Address Management²⁴ (IPAM) database; one of the three contacts was retired and one was no longer the system administrator.
- Management could not physically locate two systems identified during our scans. Seven days after our scans, management was able to locate one system identified as an idle server, and it was subsequently removed from the network. However, the other system was not physically located for more than 80 days.²⁵

These issues occurred because management did not employ uniform processes for associating administrators with specific network devices and for physically locating systems on the network. When management cannot quickly locate network devices and identify administrators, an attacker has more time to install malware, steal information, corrupt data, and disrupt operations. Additionally, management may encounter problems resolving issues and recovering operations.

IPAM automatically discovers IP address infrastructure servers on the network and enables administrators to manage them from a central interface.
 As of July 31, 2014.

Recommendations

We recommend management evaluate, test, and install critical patches and correct configuration settings on the identified databases and operating systems. We recommend the vice president, Information Technology, direct the manager, Enterprise Access Infrastructure, to:

1. Evaluate, test, and install critical patches for the 2. Configure servers and workstations to comply with information security policy for audit logs. for the firewalls. 3. Disallow 4. Remove or rename the from the databases on the Biohazard Detection Systems and change the We recommend the vice president, Engineering Systems, direct the manager, Engineering Software Management, to: 5. Evaluate, test, and install critical patches for the database systems, Windows operating systems, and Linux operating systems. 6. Configure systems connected to the intranet to comply with information security policy and configuration standards, including intrusion prevention software, antivirus protection, password complexity, and audit logging requirements. on systems that are on the Postal Service intranet. 7. Disable We recommend the vice president, area operations for Capital Metro Area, direct the district manager, Capital District, to: 8. Discontinue sharing credentials used to access the 9. Configure and patch the in accordance with Postal Service policy on an ongoing basis. We recommend the Chief Information Officer and executive vice president direct the vice president, Information Technology, to coordinate with the vice president, Engineering Systems, to: 10. Develop a uniform process for information systems management to identify the location of all systems physically connected to the network, and the administrators associated with each system.

Management's Comments

Management agreed with recommendations 1, 2, and 4 through 10, and partially agreed with recommendation 3.

Regarding recommendation 1, management created the patches to bring the systems into compliance. Solutions Development and Support and Business Relationship Management will evaluate their applications and install the patches by September 30, 2015.

Regarding recommendation 2, management stated these vulnerabilities occurred in the systems because an automated procedure used during the logon process does not configure the audit logging settings. Management is working to convert to a group policy object that will contain the proper settings. Management's target implementation date is October 1, 2015.

Regarding recommendation 3, management agreed to review the Network Connectivity Review Board request to determine if the access was approved and still appropriate, and will adjust firewall rules as needed. Management's target implementation date is March 31, 2015.

Regarding recommendation 4, management stated they removed the **second** from the **second** databases on the BDS and changed the **second** as of November 19, 2014. Management requested closure of this recommendation with the issuance of the report.

Regarding recommendation 5, management will continue to evaluate, test and install the available critical patches where applicable. An **set of the set of**

Regarding recommendation 6, management stated they will continue to evaluate information system configurations and ensure the units remain configured according to the appropriate security standards. Management stated their evaluations are continuously ongoing.

Regarding recommendation 7, management will evaluate the removal of **a case** by case basis to ensure that systems security is not put at risk and to confirm any removal does not adversely impact system maintenance or support efforts needed to ensure availability. Management's target implementation date is April 2015.

Regarding recommendations 8 and 9, management stated it has disconnected both systems from the routed network and prohibited them from being attached in the future. The IT manager will visually ensure on a continuing basis that the equipment remains disconnected. Management stated they disconnected the systems on July 24, 2014.

Regarding recommendation 10, the manager for IT will coordinate with **Systems** Systems to develop a uniform process to identify the location of all systems physically connected to the network, and the administrators associated with each system. Management's target implementation date is September 30, 2015.

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

Evaluation of Management's Comments

The OIG considers management's comments responsive to recommendations 1 through 5, 7, and 10 and corrective actions should resolve the issues identified in the report.

Regarding recommendation 6, management stated Handbook AS-805-G *Information Security for Mail Processing/Mail Handling Equipment* (March 2004) should be used for computer systems and networks that manage, monitor, and control mail processing functions. We disagree with this interpretation for the systems we reviewed. We used Handbook AS-805, *Information Security* (May 2014) because it applies to all information resources, organizations, and personnel. Specifically, Section 11-2.2 states that all equipment connected to the network must meet current Postal Service security hardening standards. Handbook AS-805-G, which is a supplement of Handbook AS-805, addresses policies and requirements that apply to the mail processing/mail handling equipment (MHE) private network environment that are not addressed in Handbook AS-805.²⁶ The systems and databases we reviewed for this audit were connected to the Postal Service routable network. Therefore Handbook AS-805 applies to these connected **systems**.

Regarding recommendations 8 and 9, we disagree that removing the system from the network will resolve the issues identified in the report. Per Handbook AS-805, Section 1-2 states Information Security applies to all information resources, organizations, and personnel. Therefore, removal of the systems from the network is not sufficient. The use of shared credentials should be discontinued and the **systems** should be configured and patched in accordance with policy.

Management requested recommendation 4 to be closed with the issuance of this report. However, management will need to provide the OIG with documentation showing the **Section** have been removed from the **Section** databases on the BDS and the **Section** have been changed before the recommendation can be closed.

The OIG considers recommendations 3, 4, 7, and 9 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	15
Background	15
Objective, Scope, and Methodology	15
Prior Audit Coverage	16
Appendix B: Configuration Management Vulnerabilities	17
Appendix C: Patch Management Vulnerabilities	19
Appendix D: Management's Comments	20

Appendix A: Additional Information

Background

The Postal Service is organized in seven geographical areas that consist of 67 districts. The Capital District, within the Capital Metro Area, delivers mail to more than 4 million residences, businesses, and Post Office boxes. During FY 2013, the Capital District processed about 2 billion pieces of mail and reported \$470.9 million in revenue. The Capital District had about 6,600 employees supported by four district information systems staff. As of the date of this report, the Capital District operated 260 facilities.

The IT infrastructure is segmented as a routable network²⁷ and a non-routable network.²⁸ The **second** workstations are on the intranet and used for administrative business, including browsing the Internet. Centralized management and control of **second** systems is conducted at the IT service center in **second**. The non-routable network supports the MPE/MHE and is not intended for Internet connections. District Information Systems managers provide local support for the **second** systems and administer the **systems**. Local support for MPE/MHE is the responsibility of Maintenance managers.

Objective, Scope, and Methodology

Our objective was to review security controls in the Postal Service's Capital District to determine whether the infrastructure adequately protects Postal Service data. To accomplish our objective, we performed enumeration to evaluate the environment residing within the Curseen-Morris Processing and Distribution Center (P&DC), Southern Maryland P&DC, Suburban Maryland P&DC, and Capital Metro Area Office.

We performed vulnerability scans between April and August of 2014, using: Our scans were performed on the routable network only. The scan results are presented in detail in Appendix B and Appendix C. We performed analysis of the systems and reported them by system type:

Table 4 identifies the 35 systems we judgmentally selected for testing, listed by operating system. Of those 35, only 33 were scanned for patch management because Postal Service management experienced difficulties identifying the appropriate administrators of the systems. In addition, only 29 systems were scanned for configuration compliance because management would have had to change the system registry configurations in order to provide us access, which would have significantly weakened system security.

²⁷ The Postal Service operates and maintains an intranet to conduct Postal Service business. An intranet is a network based on Internet technologies located within an organization's network perimeter.

²⁸ Non-routable MPE and mail processing infrastructure devices that are only connected to MPE local area networks. Systems can only communicate within the network.

Table 4. In Scope Systems

Operating System				HVAC ³²	Grand Total
	0	3	0	0	3
	1	0	0	0	1
	0	13	0	0	13
	0	2	2	0	4
	7	0	0	0	7
	2	2	0	0	4
	1	1	0	1	3
Grand Total	11	21	2	1	35
Percentage	31.4%	60.0%	5.7%	2.9%	100.0%
Source: OIG and	scanning tool results				

The OIG provided management with the raw data from the scans and a list of 354 patch vulnerabilities with 208 missing patches.

We conducted this performance audit from August 2013 through December 2014. However, we suspended the project from September 2013 to April 2014 due to higher priority audit work and to provide management time to correct issues identified during our South Florida District Vulnerability Assessment issued in October, 2013.

The audit was performed 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 objective.

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

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact
South Florida District Vulnerability Assessment	IT-AR-14-001	10/22/2013	None
Patch Management Processes	IT-AR-12-002	1/9/2012	None

³² Heating Ventilation Air Conditioning monitoring system.

Appendix B: Configuration Management Vulnerabilities

Table 5 summarizes the compliance areas the OIG reviewed to determine if Windows systems were compliant with Postal Service configuration standards.

Table 5. Configuration Compliance – Windows

Windows Systems Scanned	Compliant	Non-Compliant	Compliant	Non-Compliant	Compliant	Non-Compliant
Compliance Check ³³						
	11	0	2	0	13	0
	11	0	0	2	12	1
	11	0	0	2	5	8
	11	0	1	1	12	0
		Ū		I	12	0
	11	0	0	2	10	3
	11	0	0	2	6	
	11	0	0	2	0	1
	11	0	2	0	13	0
	9	0	0	2	12	0
	11	0	2	0	13	0
	5	6	0	2	10	3
	4	7	0	2	6	7
	3	8	0	2	4	9
	11	0	2	0	13	0
	3	8	0	2	2	11
	3	8	0	2	10	3
	3	8	0	2	11	2
	3	8	0	2	2	11
	3	8	0	2	11	2
Source: OIG scanning tool results.						

33 Security Hardening Standards for

Table 6 summarizes the compliance areas that the OIG reviewed to determine if servers running the Linux operating system were compliant with Postal Service configuration standards.

Table 6. Configuration Compliance – Linux

Linux Systems Scanned	Compliant	Non-Compliar
Compliance Check ³⁴		
	0	3
	0	3
	0	3
	0	3
	0	3
	-	-
	0	3
	3	0
	0	3
	0	3
	0	3
	0	3
	0	3
	0	3
	3	0
	3	0
	0	3
	3	0
	3	0
Source: OIG and scanning tool results.		

Appendix C: Patch Management Vulnerabilities

Table 7 summarizes the Windows and Linux operating systems critical and high-risk vulnerabilities we identified. We associated the patch vulnerabilities by product³⁵ and impact categories.³⁶ All vulnerabilities had a missing patch that was available for more than 90 days.37

Table 7. Impact of Vulnerabilities Grouped by Product

Impact Category and Product				Grand Total
Elevation of Privilege	20	2	0	22
	10	0	0	10
	10	2	0	12
Remote Code Execution	11	7	0	18
	0	1	0	1
	11	6	0	17
Undefined ³⁸	23	41	4	68
	0	3	0	3
	17	10	2	29
	0	2	2	4
	2	6	0	8
	4	4	0	8
	0	16	0	16
Grand Total	54	50	4	108

Source: OIG scanning tool results.

35 Product is the software suite or operating system identified in scan results from that have been released by the vendor within 90 days, as of June 15, 2014.

The numbers associated with the product represent the missing patches

36 Impact categories group vulnerabilities based on the type of threat. The categories are from

37 As of June 15, 2014.

38 The vulnerabilities categorized as "Undefined" by

may fit into multiple categories of impact.

Appendix D: Management's Comments





Both systems have been disconnected from the Postal Routed Network and will be prohibited from being connected in the future. The IT manager will visually ensure on a continuing basis that the equipment remains disconnected.

The OIG stated at the exit conference for this audit that they have recently attempted to ping both systems to determine if they are reachable and therefore open to risk of unauthorized access or corruption. It was determined they were not and the district is in compliance.

Target Implementation Date July 24, 2014

Responsible Official Raynard A Nowden Sr. Manager Information Systems

This report and management's response do not contain information that may be exempt from disclosure under the FOIA.

ristin A Seaver

cc: James P. Cochrane, Chief Information Officer and Executive Vice President Michael Amato, Vice President, Engineering Systems John T. Edgar, Vice President, Information Technology Kristin A. Seaver, Vice President, Capital Metro Area





POSTAL SERVICE
November 21 st , 2014
LORI LAU DILLARD DIRECTOR, AUDIT OPERATIONS (A)
SUBJECT: Response to Draft Report: Capital District Vulnerability Assessment (IT-AR-15-DRAFT)
Recommendation [1]: Evaluate, test, and install critical patches for the systems.
Management Response/Action Plan: Management agrees with this recommendation. Desktop Computing has created the patches to bring the systems into compliance. Solutions Development & Support and Business Relationship Management agree to evaluate their applications and install these patches.
Target Implementation Date: September 30, 2015
<u>Responsible Officials:</u> Manager, Solutions Development & Support, Information Technology Manager, Business Relationship Management, Information Technology
Recommendation [2]: Configure servers and workstations to comply with information security policy for audit logs.
Management Response/Action Plan: Management agrees with this recommendation. These vulnerabilities occurred in the systems because management uses automated procedures during the logon process that do not configure the correct audit logging settings. Management is working to convert from the logon process to a group policy object that will contain the proper settings.
Target Implementation Date: October 1, 2015
Responsible Official: Manager, Enterprise Access Infrastructure, Information Technology
475 L'ENFANT PLAZA SW WASHINGTON DC 20280-5000 WWW/USPS COM Page 1 of 3







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