Internal Revenue Service Databases Continue to Be Susceptible to Penetration Attacks

December 14, 2007

Reference Number: 2008-20-029

Redaction Legend:

2(f) = Risk Circumvention of Agency Regulation or Statute (whichever is applicable)
3(d) = Identifying Information - Other Identifying Information of an Individual or Individuals

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

December 14, 2007

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: *(for)* Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Internal Revenue Service Databases Continue to Be Susceptible to Penetration Attacks (Audit # 200720017)

This report presents the results of our review to determine whether databases used by Internal Revenue Service (IRS) computer applications are secure from exploitation by unauthorized individuals. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2007 Annual Audit Plan and was part of the Information Systems Programs unit's statutory requirements to annually review the adequacy and security of IRS technology.

Impact on the Taxpayer

The IRS continues to have recurring information security weaknesses that make its databases susceptible to penetration attacks. Because the IRS stores its taxpayer, financial, and other data in more than 2,100 databases, attacks on these databases could result in taxpayer identity theft and fraud. Such attacks could also result in financial losses to the Federal Government.

Synopsis

Since March 2003, we have identified and reported significant weaknesses in IRS database security controls. Our previous reviews have demonstrated that control weaknesses could be exploited to gain access to sensitive taxpayer information and disrupt IRS computer operations. Although we did not exploit the vulnerabilities during this review, we found the security weaknesses remain. We are very concerned that these high-risk weaknesses continue to exist and that greater efforts have not been taken to correct them.

To ease the installation process, vendors typically ship database software with installation accounts that contain the same (default) logon and same password. In some cases, the password

is blank. The IRS requires that these passwords be immediately changed after database installation. During this review, we tested more databases than in prior reviews for the existence of default or blank passwords for installation accounts. Based on our scans of IRS networks, we determined that 11 percent of the approximately 1,900 databases scanned had 1 or more installation accounts with a default or blank password. A total of 369 installation accounts had default or blank passwords; 26 contained powerful database administrator privileges. Malicious users can exploit accounts with default or blank passwords to steal taxpayer identities and carry out fraud schemes. Databases found with default or blank passwords during our scans include those that contain personally identifiable tax information.

These password weaknesses continue to exist because of deficiencies in the IRS' process for identifying and resolving them. The IRS Computer Security Incident Response Center conducts monthly scans to detect default and blank database passwords. While the Center identifies password weaknesses on the systems it scans, it does not adequately scan all IRS databases. The process for reviewing these scan results has resulted in the correction of many weaknesses. However, we identified deficiencies in the process that hamper the effectiveness of the IRS team tasked with correcting these weaknesses.

Changing default and blank passwords after database installation is a fundamental security rule that all database administrators should know to follow. We have repeatedly apprised the IRS of this issue, and it has taken actions to publish standards and identify and correct these password weaknesses. Because these actions have resulted in only limited success, we conclude that default and blank database passwords continue to exist because managers and employees are not taking seriously their responsibilities for implementing secure databases. Consequently, the IRS needs to take stronger actions to ensure employees take these responsibilities seriously.

We also found that a majority of the IRS databases scanned do not have the latest software updates (patches) installed. Our scans found 65 percent of the databases scanned needed to be updated, with more than 300 databases being outdated from 11 months to 20 months. As a result, outdated IRS databases were collectively susceptible to nearly 40,000 database vulnerabilities, one-half of which are considered high risk. These vulnerabilities include those used for common penetration attacks. IRS standard database security configurations require that database software be kept current with the most recent software updates. These updates protect computer software from emerging vulnerabilities that can be used to attack it and gain access to its data.

Although the IRS is adequately identifying appropriate patches for its databases, installation of the patches is not currently being monitored and there is no automated tool available to detect whether patches have been installed.

Recommendations

We recommended the Chief Information Officer ensure security training is provided to employees with key security responsibilities and coordinate with other heads of office to emphasize the need for disciplinary actions for managers and employees who fail to fulfill their security responsibilities. The Chief Information Officer should improve the process for identifying and correcting accounts with blank or default passwords by expanding the scanning criteria, analyzing the Computer Security Incident Response Center scan results, and changing the methodology for determining repeat findings. In addition, the Chief Information Officer should establish a process for monitoring database patch installations and updates to current versions of database software.

Response

IRS management agreed with all of our recommendations. The Associate Chief Information Officer, Cybersecurity, will update the security training curriculum and courseware to specifically include the need to change default and blank passwords and will prepare a memorandum reemphasizing the need for disciplinary action for managers and employees who are not fulfilling their security responsibilities. The Computer Security Incident Response Center will implement and expand a quarterly database scanning component to its vulnerability management program. The Cybersecurity organization will expand scanning efforts to include computer names and other identifiable information needed to efficiently resolve password weaknesses, disseminate scan results to appropriate parties, trend scan results to detect repeat offenders, track and report quarterly on the status to those employees responsible for correcting default and blank passwords, and purchase database vulnerability scanning software to detect the absence of needed security patches on IRS databases. Management's complete response to the draft report is included as Appendix VII.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Abbreviations

CSIRC	Computer Security Incident Response Center
IRS	Internal Revenue Service
2(f)	2(f)

Background

The Internal Revenue Service (IRS) is responsible for maintaining security over computer systems that process more than $2 trillion in receipts and $11 billion in expenditures. These systems must maintain the privacy of tax information for about 134 million taxpayers. The IRS stores its taxpayer, financial, and other data in more than 2,100 databases. Due to the sensitivity of these data, the IRS could be a target for malicious users intent on committing identity theft and fraud. Theft of the data on these systems could also result in financial losses to the Federal Government. Because the IRS has many employees and contractors with access to its networks, it is vulnerable to insider theft of its confidential data.

While computer security is typically applied in layers around a computer system, the last and possibly best line of defense in protecting IRS data are database security controls. However, our prior audits have identified significant weaknesses in IRS database security controls. Most recently, we reported that standard database security configurations have not been effectively implemented on IRS databases.[1] In addition, our previous penetration tests have demonstrated that control weaknesses could be exploited to gain access to sensitive taxpayer information and disrupt IRS computer operations.[2]

We conducted this review to determine whether two key control weaknesses identified in our September 2005 penetration test report had been corrected. We tested more databases than in our previous penetration tests for the existence of default or blank passwords for installation accounts, but we did not attempt to exploit the weaknesses. This review was performed at the IRS National Headquarters in Washington, D.C., in the Offices of the Chief Information Officer during the period May through August 2007.

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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[1] *Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation* (Reference Number 2007-20-129, dated August 22, 2007).
[2] See Appendix IV for the list of prior penetration test reports.

Results of Review

The issues presented in this report are recurring information security weaknesses that the IRS has been unable to correct. We are very concerned that these high-risk weaknesses continue to exist and that greater efforts have not been taken to address and correct them.

Database Accounts With Default or Blank Passwords Continue to Be Found

To ease the installation process, vendors typically ship database software with installation accounts that contain the same (default) logon and same password. In some cases, the password is blank. For example, 2(f) databases use "SA" as a common logon for database administrators and leave the password blank. 2(f) databases contain similar logons and passwords that are readily available from the Internet. Database software can have hundreds of installation accounts with default logons and passwords, with varying degrees of database privileges. The most powerful accounts are database administrator accounts, which have powerful privileges that can be used to access the entire database. These accounts are particularly risky because they provide the user with the capability to change configurations, add user accounts, and take other actions that could be used for malicious purposes. Accordingly, vendors recommend and the IRS requires that, after an administrator accesses the database for the first time, he or she change the logons and passwords to ones that cannot be easily guessed.

Since March 2003, we have issued three reports on our efforts to penetrate IRS computer systems, all of which identified database administrator accounts with blank or default passwords as high-risk weaknesses. The prior penetration test reports are listed in Appendix IV. In our most recent penetration test report, we recommended the IRS change the weak logons and passwords on accounts we identified, enforce accountability, and increase security awareness of its administrators to ensure blank and default passwords are changed during installation. In response, IRS management agreed to correct the weaknesses we identified, perform monthly vulnerability scans, establish a review board to improve processes and to ensure disciplinary actions are consistent when requirements are not met, and provide awareness training to administrators. By March 2006, the IRS reported that identified passwords had been corrected. During this review, we confirmed that monthly vulnerability scans were being performed and the review board was in place. However, we could not obtain support that IRS employees with key security responsibilities had been identified and provided security training on the correct installation procedures for database software.

The actions taken to date have not been sufficient because the IRS continues to have difficulty ensuring default and blank database passwords are not used. We scanned IRS networks and determined that 11 percent of the approximately 1,900 databases scanned had 1 or more installation accounts with default or blank passwords. We found a total of 369 installation accounts with default or blank passwords. Of these, 26 accounts had powerful database administrator privileges. Appendix V provides additional details on the results of our tests.

Malicious users can exploit accounts with default or blank passwords to steal taxpayer identities and carry out fraud schemes. In addition, because multiple users can use the accounts, it is difficult to establish accountability for actions taken. For production systems, application developers can exploit default or blank passwords to access production databases for their application. Once inside, developers can make changes to production databases and applications that are unauthorized and untested, resulting in unexpected consequences such as breaking application functionality or preventing its use.

While we did not attempt to exploit default or blank passwords to gain access to IRS databases in this review, attempts in our previous penetration audits have been successful. In the September 2005 penetration test report, database administrator accounts with default or blank passwords were used to gain access to employee, taxpayer, and corporate tax forms. We have also demonstrated in the prior penetration reports that, once access is gained to the administrative accounts for a database, a malicious user can elevate those privileges to other databases and operating systems, gaining access to even more taxpayer accounts. Accordingly, the IRS should have no tolerance for accounts with default and blank passwords.

We attempted to associate IRS applications with the databases we found to assess the effect on the IRS in the event these applications were compromised. Using information obtained during our scans and available IRS resources, we were able to identify applications for less than one-half of the databases found. On May 25, 2007, we asked the IRS to identify the remaining applications and confirm the applications we were able to identify through research. However, the IRS has been unable to fully provide this information, most likely because it does not have a comprehensive source of information for its applications and their associated databases. Some of the applications we were able to identify with default or blank database passwords are shown in Table 1.

Table 1: Applications Found With Default or Blank Database Passwords

Application	Description	Tax Data Residing on Systems With Blank or Default Passwords
2(f)		

Sources: Treasury Inspector General for Tax Administration scans of the IRS network, systems descriptions from IRS Intranet web sites, and discussions with IRS personnel.

Installation database accounts with default or blank passwords continue to exist because of deficiencies in the IRS' process for identifying and resolving these password weaknesses. In response to our September 2005 penetration test report, the IRS Computer Security Incident Response Center (CSIRC) began scanning IRS networks for default and blank passwords, with the results being forwarded to a review team for correction. This review team is comprised of representatives from divisions within the Modernization and Information Technology Services organization, with oversight by the Enterprise Networks organization.

To detect default and blank database passwords, the CSIRC conducts monthly scans of IRS databases. While the CSIRC identifies password weaknesses on the systems it scans, it does not adequately scan all IRS databases. Specifically, we found:

- Only two types of database software are scanned. The database software scanned are among the types most prevalently used by the IRS. However, the IRS uses more than 30 different types of database software.
- Only two ports (network connections) are scanned. Users can access databases on many different ports.

- Only a few installation account and password combinations are tested. Some database software packages have hundreds of these combinations.

If we had limited our scans to the criteria used by the IRS, we would have found only 64 accounts, instead of the 369 accounts. During our review, the CSIRC modified its scan criteria to incorporate additional ports and installation account and password combinations.

The process for reviewing the CSIRC's scan results has resulted in the correction of many default and blank database passwords. According to the Enterprise Network organization review team's monthly status reports from December 2006 through April 2007, 30 percent of the password weaknesses addressed by the review team resulted in corrections. In addition, most of the weaknesses addressed by the review team did not reappear on the subsequent months' reports. However, we found deficiencies in this process that hamper the effectiveness or reporting accuracy of the review team's efforts.

- Inadequate Oversight: While the CSIRC password scan results are sent to the review team, not all weaknesses are reviewed. We reviewed status reports from the review team from December 2006 through July 2007 and, until April 2007, computers identified in the CSIRC's 2(f) database password scans were generally included in the team's status reports, with a few exceptions. However, no CSIRC scan results for May through July 2007 were included. We discussed these omissions with Enterprise Networks organization personnel, who informed us the review team does not directly review the CSIRC scan results but reviews them as part of their monthly status report documents. 3(d) In addition, the review team did not provide sufficient oversight to ensure CSIRC scan results were accounted for.

- Inadequate Reporting of Repeat Findings: The review team identifies computers appearing in consecutive months as repeat findings. They identify repeat findings as "second occurrences" and generally look only at the preceding month's report to identify them. However, this methodology understates the number of repeat findings and precludes the IRS from identifying employees warranting disciplinary actions. From December 2006 through April 2007, the review team identified 80 computers as repeat findings. However, our review of the status reports over the same period identified 129 repeat findings. Many of the discrepancies were a result of computers appearing in nonconsecutive months. Also, reporting repeat findings as "second occurrences" does not provide sufficient information to identify problem areas. If the reports identified a running total of repeat occurrences, the review team could more easily identify organizations and personnel that need additional training or disciplinary actions to ensure password weaknesses do not occur. We found several computers that appeared in each of the five monthly status reports.

- Insufficient Information: Scan results forwarded by the CSIRC do not include all information needed to timely identify the computers on which the weaknesses were found. In particular, computer names are not included, only network addresses. Because network addresses can change, computer names are also needed.

Changing default and blank passwords after database installation is a fundamental security rule that all database administrators should know to follow. We have repeatedly apprised the IRS of this issue. The IRS has published standard database security configuration standards addressing this weakness and established processes for identifying and correcting installation default password weaknesses. Because these actions have resulted in only limited success in resolving this issue, we conclude that default and blank database passwords continue to exist in part because managers and employees are not taking seriously their responsibilities for implementing secure databases. Consequently, the IRS needs to take stronger actions.

Recommendations

The Chief Information Officer should:

Recommendation 1: Implement the previously stated corrective action to identify employees with key security responsibilities and provide security training to these employees, specifically on default and blank passwords.

> ***Management's Response:*** IRS management agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will update the existing security training curriculum and courseware to specifically include the need to change default and blank passwords.

Recommendation 2: Coordinate with other heads of office to emphasize the need for disciplinary actions for managers and employees who are not fulfilling their security responsibilities, as evidenced by repeat findings of failure to comply with IRS security configuration requirements for servers, databases, and other computing platforms. Specific emphasis is needed to ensure default and blank passwords are removed for database administrator accounts placed into operation.

> ***Management's Response:*** IRS management agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will prepare a memorandum reemphasizing the need for disciplinary action, as appropriate, for managers and employees who are not fulfilling their security responsibilities.

Recommendation 3: Expand the criteria used for scanning IRS databases for the presence of administrator accounts with default or blank passwords. These criteria should encompass additional database software used by the IRS, a broader range of account and password combinations, and additional ports in which databases can be accessed. In addition, CSIRC scan

results should be expanded to include computer names and other identifiable information needed to more quickly resolve password weaknesses.

> ***Management's Response:*** IRS management agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will implement and expand a quarterly database scanning component to the vulnerability management program. The Cybersecurity organization will expand scan efforts to include computer names and other identifiable information needed to efficiently resolve password weaknesses. In the near term, the Cybersecurity organization will purchase the technology, establish processes for conducting scans, and expand parameters of current testing capabilities.

Recommendation 4: Ensure the employees responsible for correcting default and blank passwords directly review the CSIRC scan results. In addition, the methodology for determining repeat findings should be modified to include running totals for computers identified on multiple scans.

> ***Management's Response:*** IRS management agreed with this recommendation. The Associate Chief Information Officer, Cybersecurity, will ensure dissemination of scan results to appropriate parties and trending of scan results to detect repeat offenders. The Cybersecurity organization will also track and report quarterly on the status to those employees responsible for correcting default and blank passwords. Until the solution is fully implemented, it will purchase the technology and establish processes for conducting and reviewing scans.

Databases Are Not Adequately Updated to Protect Against Emerging Vulnerabilities

In the September 2005 penetration test report, we identified computers susceptible to several high-risk operating system, database, and web server attacks. In some instances, operating system vulnerabilities were used to gain access to the computer, providing full access to all of the computer files. The computers were susceptible because software updates to protect against the vulnerabilities were not installed. Some computers were also found to be running outdated versions of the operating system. We also previously reported weaknesses with the IRS' software patching process,[3] although database software was not specifically assessed.[4] Given the findings in these prior reports, we focused this review on assessing how susceptible IRS databases were to database-specific vulnerabilities.

[3] A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.

[4] *Uninstalled Computer Security Patches Continue to Put Computer Systems at Risk* (Reference Number 2006-20-167, dated September 21, 2006).

IRS standard database security configurations specify that database software should be kept current with the most recent software updates. These updates protect computer software from emerging vulnerabilities that can be used to attack it and gain access to its data. Updates can be provided in the form of a patch, which fixes a specific vulnerability, or by installing a new software version.

Our scans of the IRS network found that 1,242 (65 percent) of the nearly 1,900 databases scanned need to be updated. These databases were not operating at the current database software version as of March 2007, the date our software scanner was last updated. Because our scans were conducted in May 2007, these databases were outdated for at least 2 months, with more than 300 databases found to be outdated from 11 months to 20 months.

In addition, over one-third of the databases' versions were so out of date that the manufacturer no longer provides security patches or other updates. Our scans found 45 outdated database versions for the 5 types of database software we tested. Appendix VI provides additional details on the results of our tests.

As a result, outdated IRS databases were collectively susceptible to nearly 40,000 database vulnerabilities, one-half of which are considered high risk. These vulnerabilities include those used for common penetration attacks.[5] Malicious users could use one or more of these attack methods to gain access to IRS databases, potentially providing unauthorized access to taxpayer information, corrupting data, and shutting down the databases.

We reviewed the IRS process for identifying patches and monitoring their implementation. The IRS is adequately identifying database patches for its database software. The CSIRC is primarily responsible for identifying available patches and notifying IRS functions of these patches and related vulnerabilities. We reviewed the CSIRC patch inventory and found it adequately identified current patches for the database software used by the IRS.

However, installation of database patches is not currently being monitored. The CSIRC requires in its critical patch advisories that persons responsible for patching affected systems report the status of patch installation to the CSIRC. However, CSIRC personnel informed us they do not receive status information on database patch installations. This may be in part due to the lack of notice of this requirement or method for reporting patch status on the CSIRC's web site. The CSIRC has not aggressively followed up with those organizations required to implement patches.

In addition, automated tools are not available to detect whether database patches or current software versions have been implemented. The IRS does track the status of patches for computer operating systems. However, the scans are able to identify patches only for specific operating systems, not databases.

[5] See Appendix VI for descriptions of these attack methods.

The process of implementing database updates in the IRS is complex because many IRS organizations are involved in the process. Therefore, due to the amount of testing required to identify specific reasons why updates are not installed, we plan to further examine the processes for updating database software in our Fiscal Year 2008 audits.

In general, though, we believe one of the primary reasons why databases are not updated is reluctance by administrators to install patches because of a concern that they may otherwise impair the application being patched. In our September 2006 patching report, we reported a similar reluctance for installation of operating system patches.

Recommendation

Recommendation 5: The Chief Information Officer should establish a process for monitoring database patch installations and updates to current versions of database software. This process should make use of automated scans or other tools where possible to verify the patches and updates are installed.

> ***Management's Response:*** IRS management agreed with this recommendation. The Cybersecurity organization will purchase database vulnerability scanning software to detect the absence of needed security patches on IRS databases. Until the solution has been fully implemented, it will use patch advisories to reemphasize the methods for reporting patch status to the CSIRC.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of our review was to determine whether databases used by IRS computer applications are secure from exploitation by unauthorized individuals. To accomplish this objective, we:

I. Prepared for scanning the IRS databases.

A. Obtained software and computer equipment/hardware needed to perform discovery and audit scanning of the IRS databases.

B. Developed customized database scanning policies to identify potential database vulnerabilities.

C. Reviewed IRS criteria for database passwords and software updates (Internal Revenue Manual Section 10.8.4).

II. Identified the population of databases used by the IRS.

A. Identified the range of network, or internet protocol, addresses used by the IRS. The scope included IRS networks as well as networks for the Appeals Division; Office of Research, Analysis, and Statistics organization; Criminal Investigation Division; and Office of Chief Counsel. Only addresses confined within the IRS were examined.

B. Scanned the selected network address ranges using the AppDetective scanning software. 2(f) 2(f) Network ranges assigned to IRS servers were primarily scanned, along with additional ranges assigned to workstations and other devices.

III. Determined whether exploitable vulnerabilities were present on selected IRS databases.

A. Scanned 2(f) databases to identify default or blank database account passwords.

B. Scanned 2(f) databases to identify software updates. The scanning software we used was unable to scan 2(f) databases for software updates.

IV. Identified causes for the existence of exploitable vulnerabilities.

A. Analyzed the scan results to determine whether common vulnerabilities were present.

B. Evaluated the IRS processes for identifying and correcting default and blank passwords.

C. Determined whether causes identified in the report *Uninstalled Computer Security Patches Continue to Put Computer Systems at Risk* (Reference Number 2006-20-167, dated September 21, 2006) applied to database patching issues.[1] We reviewed the IRS process for identifying database software updates and monitoring their implementation. We did not review the process for implementing software updates due to the complexity of the process for implementing databases and the numerous IRS organizations involved. Therefore, due to the amount of testing required to identify specific reasons why updates are not installed, we plan to further examine the processes for updating database software in our Fiscal Year 2008 audits.

D. Determined whether blank or default passwords have been previously identified and reported by the CSIRC.

V. Assessed the effect of the exploitable vulnerabilities found.

A. Assessed the access levels for accounts found to have blank or default passwords.

B. Assessed the severity of the databases that had not been adequately updated.

C. Identified the IRS business risk by identifying the applications associated with vulnerable databases.

[1] A patch is a fix of a design flaw in a computer program. Patches must be installed or applied to the appropriate computer for the flaw to be corrected.

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen Mullins, Director
Michelle Griffin, Audit Manager
Michael Howard, Lead Auditor
Charles Ekunwe, Senior Auditor
Jacqueline Nguyen, Senior Auditor
Stasha Smith, Senior Auditor

Appendix III

Report Distribution List

Acting Commissioner C
Office of the Commissioner – Attn: Acting Chief of Staff C
Deputy Commissioner for Operations Support OS
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
    Chief Information Officer OS:CIO
    Director, Program Oversight OS:CIO:SM:PO

Appendix IV

Prior Penetration Test Reports

This report is the fourth since March 2003 to identify weaknesses resulting from penetration tests of IRS networks and computer systems. The prior reports are:

- *Internal Penetration Test of the Internal Revenue Service's Networked Computer Systems* (Reference Number 2005-20-144, dated September 2005).
- *Penetration Test of Internal Revenue Service Computer Systems* (Reference Number 2004-20-073, dated April 2004).
- *Penetration Test of Internal Revenue Service Computer Systems* (Reference Number 2003-20-082, dated March 2003).

Appendix V

Additional Password Test Information

This appendix provides additional information on the blank and default installation account passwords found on IRS databases. Our assessment included scanning five types of databases for these passwords. Table 1 summarizes the results by database type.

Table 1: Types of Databases Found With Blank and Default Passwords

Database Type	Databases Found With Blank and Default Passwords	Databases Tested	Percentage With Blank and Default Passwords
2(f)			
Totals	**198**	**1,858**	**10.7%**

Source: Treasury Inspector General for Tax Administration assessment of selected IRS databases using data collected from scans of IRS databases.

Most IRS databases are found on the main IRS network. However, the networks for the Office of Chief Counsel and the Criminal Investigation Division are separate from the main network and are managed by each organization. Table 2 summarizes the results by the networks we scanned.

Table 2: Networks in Which Databases Were Found With Blank and Default Passwords

Network	Databases Found With Blank and Default Passwords	Databases Tested	Percentage With Blank and Default Passwords
IRS main network	196	1,745	11.2%
Chief Counsel	2	52	3.8%
Criminal Investigation	0	61	0.0%
Totals	**198**	**1,858**	**10.7%**

Source: Treasury Inspector General for Tax Administration assessment of selected IRS databases using data collected from scans of IRS databases.

Our scans found installation database accounts with default and blank passwords on production and nonproduction databases. Nonproduction databases include those used for development of applications and, in a few instances, for building databases. While nonproduction databases generally do not store taxpayer information, blank or default passwords could still be exploited to obtain sensitive information such as business rules and application programs.

Appendix VI

Additional Patch Test Information

This appendix provides additional information on the databases we identified that were not updated with the most recent patches or upgraded to the current database software versions. These versions were current as of March 23, 2007, when our scanning software was last updated. Our assessment included scanning four types of databases for current patches. Table 1 summarizes the results by database type.

Table 1: Types of Databases Found Without Current Patches

Database Type	Databases Found Without Current Patches	Databases Tested	Percentage Without Current Patches
2(f)	137	194	71%
	11	17	65%
	700	919	76%
	394	774	51%
Totals	**1,242**	**1,904**	**65%**

Source: Treasury Inspector General for Tax Administration assessment of selected IRS databases using data collected from scans of IRS databases.

Most IRS databases are found on the main IRS network. However, the Office of Chief Counsel and the Criminal Investigation Division keep their networks and systems separate from the rest of the IRS. Table 2 summarizes the results by the networks we scanned.

Table 2: Networks in Which Databases Were Found Without Current Patches

Network	Databases Found Without Current Patches	Databases Tested	Percentage Without Current Patches
IRS main network	1186	1,795	66%
Chief Counsel	19	49	39%
Criminal Investigation	37	60	62%
Totals	**1,242**	**1,904**	**65%**

Source: Treasury Inspector General for Tax Administration assessment of selected IRS databases using data collected from scans of IRS databases.

Our scans identified 45 outdated database software versions that require patches or updates. These database versions are listed in Table 3.

Table 3: Database Software Versions Found

Version Found	Current Version	Network			Totals
		IRS Main	Criminal Investigation	Chief Counsel	
2(f)					
2(f)		16	0	0	16
		3	0	0	3
		32	0	0	32
		3	0	0	3
		1	0	0	1
		82	0	0	82
2(f)					
2(f)		1	0	0	1
		1	0	0	1
		1	0	0	1
		1	0	0	1
		5	0	0	5
		1	0	0	1
		1	0	0	1
2(f)					
2(f)		2	0	0	2
		60	0	0	60
		168	0	0	168
		1	0	0	1
		1	0	0	1
		10	0	0	10
		5	0	0	5
		185	0	0	185
		17	0	0	17
		1	0	0	1

Version Found	Current Version	Network			Totals
		IRS Main	Criminal Investigation	Chief Counsel	
2(f)		11	0	0	11
		47	0	0	47
		43	0	0	43
		67	0	0	67
		0	0	2	2
		46	0	0	46
		17	0	0	17
		17	0	0	17
	2(f)				
2(f)		1	0	0	1
		4	1	0	5
		19	0	0	19
		1	0	0	1
		29	3	1	33
		107	11	5	123
		88	11	11	110
		28	0	0	28
		41	4	0	45
		1	6	0	7
		1	0	0	1
	2(f)				
2(f)		1	1	0	2
		15	0	0	15
		4	0	0	4
Grand Total		**1,186**	**37**	**19**	**1,242**

Source: Treasury Inspector General for Tax Administration assessment of selected IRS databases using data collected from scans of IRS databases.

These databases are susceptible to various methods of attack that can result in compromise of the databases and unauthorized access to the data stored in them. These well-known attack methods include:

- Buffer Overflow: This technique exploits databases by sending more information to the database than expected, thus forcing the additional data to be stored in another part of the computer's memory. If this memory permits execution of computer commands and the excess data contain database or computer instructions, then an attacker can run malicious commands to gain access to the database.
- SQL Injection: This technique is used to manipulate web sites into sending SQL queries to a database to alter, insert, or delete data in a database.
- Privilege Escalation: This technique is used by an attacker to change the privilege level of a database process and take control of that process to bypass security controls.

Appendix VII

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

RECEIVED
NOV 16 2007

NOV 16 2007

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Arthur L. Gonzalez
Chief Information Officer

SUBJECT: Draft Audit Report – Internal Revenue Service Databases Continue to Be Susceptible to Penetration Attacks (Audit # 200720017) (i-trak # 2008-29937)

Thank you for the opportunity to review and comment on your draft audit report on the security of our databases. I appreciate that your report acknowledged the monthly scans our Computer Security Incident Response Center conducts to detect default and blank database passwords and that we are adequately identifying appropriate patches for our databases.

We take data security very seriously and recognize the risks associated with the disclosure of sensitive taxpayer data. We continue to emphasize computer security practices and update our systems, processes, and training so that employees are aware of the steps they must take to secure sensitive taxpayer data from unauthorized individuals.

We concur with your recommendations and will take appropriate corrective actions, as detailed in the attachment to this memo, to implement them. Please note that on November 2, 2007, the Associate Chief Information Officer, Cybersecurity, requested that your office consider issuing the final report under a "Limited Official Use" designation as it addresses sensitive information.

Thank you for your continued support and guidance. We look forward to working with your staff to develop appropriate measures. If you have any questions, please contact me at (202) 622-6800 or Perry Robinett, Director, Program Oversight Coordination, at (202) 283-6283.

Attachment

Draft Audit Report – Internal Revenue Service Databases Continue to Be Susceptible to Penetration Attacks (Audit # 200720017) (i-trak # 2008-29937)

RECOMMENDATION #1: The Chief Information Officer (CIO) should implement the previously stated corrective action to identify employees with key security responsibilities and provide security training to these employees, specifically on default and blank passwords.

CORRECTIVE ACTION #1: We agree with this recommendation. The Associate Chief Information Officer (ACIO), Cybersecurity initiated a National Institute of Standards & Technology-compliant Specialized Security Training Program in 2003 in response to Federal Information Security Management Act (FISMA) requirements. At that time, we identified 4,200 employees with key security responsibilities. We will update the curriculum and courseware for these employees to specifically include changing default and blank passwords.

IMPLEMENTATION DATE: July 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We monitor corrective actions monthly using the Joint Audit Management Enterprise System (JAMES).

RECOMMENDATION #2: The Chief Information Officer (CIO) should coordinate with other heads of office to emphasize the need for disciplinary actions for managers and employees who are not fulfilling their security responsibilities, as evidenced by repeat findings of failure to comply with IRS security configuration requirements for servers, databases, and other computing platforms. Specific emphasis is needed to ensure default and blank passwords are removed for database administrator accounts placed into operation.

CORRECTIVE ACTION #2: We agree with this recommendation. The ACIO, Cybersecurity will prepare a CIO memorandum to all heads of offices for distribution via the Security Services and Privacy Executive Steering Committee. The memorandum will re-emphasize the need for disciplinary action, as appropriate, for managers and employees who are not fulfilling their security responsibilities. We will coordinate the need for disciplinary actions with the labor relations staff and the National Treasury Employees Union (NTEU).

IMPLEMENTATION DATE: February 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We will assess our progress during periodic monitoring activities that support the annual FISMA review. We expect to issue the memorandum before the FISMA scheduled completion date of July 1, 2008.

RECOMMENDATION #3: The Chief Information Officer should expand the criteria used for scanning IRS databases for the presence of administrator accounts with default or blank passwords. These criteria should encompass additional database software used by the IRS, a broader range of account and password combinations, and additional ports in which databases

can be accessed. In addition, CSIRC scan results should be expanded to include computer names and other identifiable information needed to more quickly resolve password weaknesses.

CORRECTIVE ACTION #3: We agree with this recommendation. Cybersecurity's Computer Security Incident Response Center (CSIRC) will implement and expand a quarterly database-scanning component to its vulnerability management program. We will use Application Security, Inc.'s DBProtect, which is the same technology the Treasury Inspector General for Tax Administration uses. In addition, we will expand CSIRC scan results to include computer names and other identifiable information needed to efficiently resolve password weaknesses.

Implementing this enterprise-wide solution will require one year. In the near term, Cybersecurity will purchase the technology and establish processes for conducting scans. In addition, we are expanding the parameters of our current testing capabilities to minimize the problem.

IMPLEMENTATION DATE: October 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We will monitor corrective actions monthly using JAMES.

RECOMMENDATION #4: The Chief Information Officer should ensure the employees responsible for correcting default and blank passwords directly review the CSIRC scan results. In addition, the methodology for determining repeat findings should be modified to include running totals for computers identified on multiple scans.

CORRECTIVE ACTION #4: We agree with this recommendation. The dissemination of scan results to appropriate parties and trending of scan data to detect repeat offenders will be a core component of the CSIRC Vulnerability Management Program. In addition, CSIRC will track and report quarterly on the status to those employees responsible for correcting default and blank passwords.

As noted in our corrective action to recommendation #3, this is a substantial issue that will require an enterprise-wide solution. In the near term, Cybersecurity will purchase the technology and establish processes for conducting and reviewing scans.

IMPLEMENTATION DATE: December 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We will monitor corrective actions monthly using JAMES.

Draft Audit Report – Internal Revenue Service Databases Continue to Be Susceptible to Penetration Attacks (Audit # 200720017) (i-trak # 2008-29937)

RECOMMENDATION #5: The Chief Information Officer should establish a process for monitoring database patch installations and updates to current versions of database software. This process should make use of automated scans or other tools where possible to verify the patches and updates are installed.

CORRECTIVE ACTION #5: We agree with this recommendation. The CSIRC deployment and quarterly scans will use Application Security, Inc.'s database vulnerability scanner, DBProtect, to detect the absence of needed security patches on IRS databases.

This issue also requires an enterprise-wide solution. In the near term, Cybersecurity will purchase the technology and establish processes for conducting and reviewing scans. We will minimize the problem by using patch advisories to re-emphasize the methods for reporting patch status to CSIRC, including reporting statuses on CSIRC's web site, until we implement the enterprise solution.

IMPLEMENTATION DATE: December 1, 2008

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We will monitor corrective actions monthly using JAMES.