Memorandum from the Office of the Inspector General

July 19, 2017

Scott D. Self, SP 3A-C

REQUEST FOR MANAGEMENT DECISION – AUDIT 2016-15369 – CYBER SECURITY PATCH MANAGEMENT OF HIGH-RISK DESKTOPS AND LAPTOPS

Attached is the subject final report for your review and management decision. You are responsible for determining the necessary actions to take in response to our findings. Please advise us of your management decision within 60 days from the date of this report.

If you have any questions or wish to discuss our findings, please contact Michael P. Anderson, Senior Auditor, at (865) 633-7393 or Scott A. Marler, Director (Acting), Information Technology Audits, at (865) 633-7352. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)
ET 3C-K

MPA:BSC
Attachment
cc (Attachment):
TVA Board of Directors
Andrea S. Brackett, WT 5D-K
Janet J. Brewer, WT 7C-K
Robertson D. Dickens, WT 9C-K
William D. Johnson, WT 7B-K
Dwain K. Lanier, MR 6D-C
Justin C. Maierhofer, WT 7B-K
Richard W. Moore, ET 4C-K
Philip D. Propes, MP 2C-C
Douglas E. Roelofs, MP 3B-C
Anthony M. Smith, MP 2H-C
Mark G. Spivey, MP 5C-C
John M. Thomas III, MR 6D-C
OIG File No. 2016-15369

Office of the Inspector General

Audit Report

To the Vice President and
Chief Information Officer,
Information Technology

CYBER SECURITY PATCH MANAGEMENT OF HIGH-RISK DESKTOPS AND LAPTOPS

Audit Team
Michael P. Anderson
Jessie A. Bradford
Weston J. Shepherd

Audit 2016-15369
July 19, 2017

ABBREVIATIONS

AD	Active Directory
FISMA	Federal Information Security Management Act
IT	Information Technology
SCCM	System Center Configuration Manager
SPEAR	Security Patch Evaluation and Rating
TVA	Tennessee Valley Authority

TABLE OF CONTENTS

APPENDICES

Audit 2016-15369 – Cyber Security Patch Management of High-Risk Desktops and Laptops

EXECUTIVE SUMMARY

Why the OIG Did This Audit

Patching has been an area of concern in previous Federal Information Security Management Act audits conducted by our office in 2014 and 2016. Findings on these audits led us to review the overall effectiveness of the Tennessee Valley Authority's (TVA) patch management process. Specifically, we chose the effectiveness of patch management for high-risk, end-user desktops and laptops as they are most vulnerable to spear phishing, a very common tactic used in today's environment to infiltrate computer networks and spread malware.

TVA utilizes two tools for managing patches of desktops and laptops. The first is Microsoft's System Center Configuration Manager (SCCM), which manages Windows operating system patches. The second is Flexera Software's Secunia, which reports on missing application patches. Active Directory is the system used to group and manage users and computers.

What the OIG Found

We found the effectiveness of TVA's cyber security patching for high-risk, end-user desktops and laptops could be improved. Specifically, we found (1) TVA is at potential risk for compromise as the patching status was unknown for 12 percent of desktops and laptops in our sample due to desktops and laptops not being managed in patch management tools; (2) 1 of 162 desktops and laptops tested had a missing patch that could lead to remote code execution that has a public exploit available; and (3) the patching process for Mac desktops and laptops is not formally documented.

What the OIG Recommends

We recommend the Vice President and Chief Information Officer, Information Technology:

1. Identify and remediate any desktops and laptops not currently managed in SCCM and/or Secunia.
2. Implement a process to ensure all corporate desktops and laptops are being managed in SCCM and Secunia.
3. Formally document the process used to manage Mac software patches in accordance with Information Technology Standard Program and Process 12.004, Information Technology Patch and Vulnerability Management.

TVA Management's Comments

In response to our draft audit report, TVA management agreed with our findings and recommendations. See Appendix B for TVA management's complete response.

BACKGROUND

Security patching has been an area of concern in previous Federal Information Security Management Act (FISMA) audits conducted by our office. In our 2014 FISMA audit,[1] we found patching timeliness for Security Patch Evaluation and Rating (SPEAR) alerts[2] were not tracked appropriately. In our 2016 FISMA audit,[3] we were unable to test the patch management process because it had not been fully implemented. These findings led us to conduct an audit of the overall effectiveness of the Tennessee Valley Authority's (TVA) patch management process. Specifically, we chose the effectiveness of patch management for high-risk, end-user desktops and laptops as they are most vulnerable to spear phishing, a very common tactic used in today's environment to infiltrate computer networks and spread malware.

Spear phishing is an advanced, persistent threat that relies on social engineering techniques and publicly available information to craft e-mails that are sent to targeted groups in a selected organization and allows attackers to gain corporate credentials or personal credentials. The information obtained through spear phishing can allow attackers to create backdoors into the corporate networks, launch attacks on business systems or personal systems, initiate denial of service, masquerade for man-in-the-middle attacks,[4] perform privilege escalation, negatively impact production, negatively impact finances or financial goals, and impact logical and physical safety.

TVA utilizes two tools for managing patches of desktops and laptops. The first is Microsoft's System Center Configuration Manager (SCCM), which manages Windows operating system patches. The second is Flexera Software's Secunia, which reports on missing application patches. Active Directory (AD) is the system used to group and manage users and computers.

See Appendix A for our objective, scope, and methodology.

FINDINGS

We found the effectiveness of TVA's cyber security patching for high-risk, end-user desktops and laptops could be improved. Specifically, we found (1) TVA is at potential risk for compromise as the patching status was unknown for 12 percent of desktops and laptops in our sample due to desktops and laptops not being managed in patch management tools; (2) 1 of 162 desktops and laptops tested had a missing patch that could lead to remote code execution that has a public exploit available; and (3) the patching process for Mac desktops and laptops is not formally documented.

---

1 Audit Report 2014-15059, Federal Information Security Management Act Evaluation, January 13, 2015.

2 SPEAR is a process TVA uses to evaluate and categorize security patches before installation.

3 Audit Report 2016-15407, Federal Information Security Management Act, January 11, 2017.

4 Man-in-the-middle attacks occur when an unauthorized party intercepts communications between two parties and can alter the communication from one party before it is sent to the second party.

TVA AT POTENTIAL RISK FOR COMPROMISE DUE TO DESKTOPS AND LAPTOPS NOT BEING IN PATCH MANAGEMENT SYSTEMS

Twenty of the 162 desktops and laptops in our sample were missing from either the SCCM system used for Windows patch management, the Secunia system used for application patch management, or both due to one of the following conditions relating to machine setup in TVA's AD:

1. The machine was not found in AD,

2. The machine was in AD but missing the Windows patch management system client, or

3. The machine was in AD but had Windows patch management system discovery errors.

As a result, the 20 desktops and laptops were not being appropriately tracked and could not allow patches to be automatically applied. We did not test the patching status of the 20 desktops and laptops due to these errors. Figure 1 shows more details of the desktops and laptops that were missing from the Windows patch management and application patch management systems.

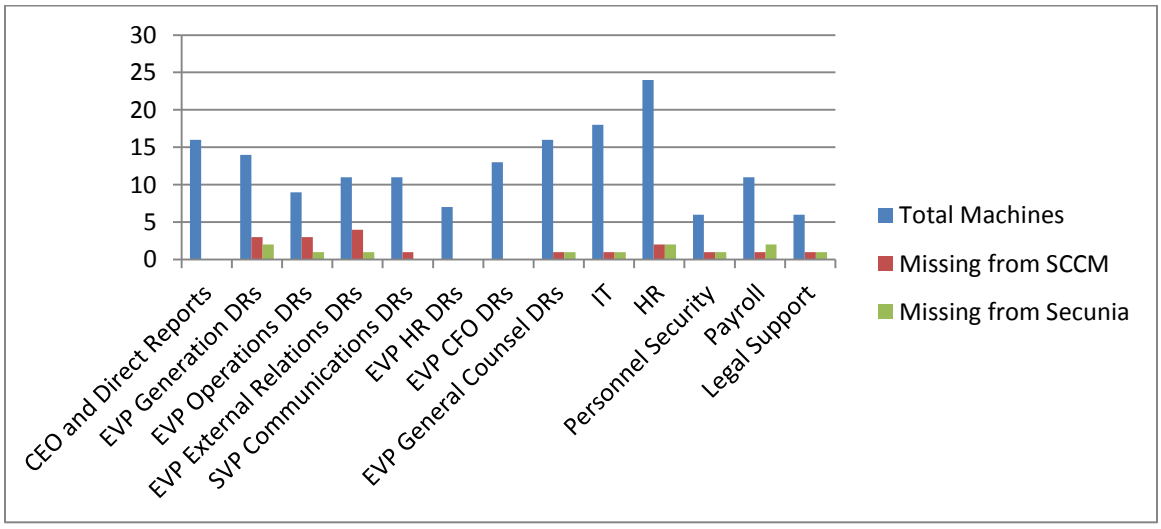

Figure 1

During our fieldwork, TVA's Information Technology (IT) management explained that the cleanup of AD records was not occurring as intended, and they have identified a remediation plan for these actions. After fieldwork was complete, TVA began the process to implement this remediation plan and provided us documentation of the process. Our review of the documentation indicated it would remediate some, but not all, of the exceptions we found.

MISSING PATCH THAT COULD LEAD TO REMOTE CODE EXECUTION WITH PUBLIC EXPLOITS AVAILABLE

We found 1 machine in the IT group that had a missing patch that could result in remote code execution with publicly available exploits. After following up with TVA's IT management to determine the cause, we were notified the issue was resolved during our fieldwork.

PATCHING PROCESS FOR MACS NOT FORMALLY DOCUMENTED

Patch management is occurring for Mac desktops and laptops in TVA; however, the process is not formally documented in work instructions. IT Standard Program and Process 12.004, Information Technology Patch and Vulnerability Management, states "Applicable work instructions will document how these patches are applied through automated tools and/or manual processes." IT Work Instruction 12.342, Windows Desktop Patch Management, documents the Windows desktop patching process. However, a similar work instruction for Mac desktops and laptops patch management has not been documented. Formal documentation of controls helps ensure consistent implementation of those controls.

RECOMMENDATIONS

We recommend the Vice President and Chief Information Officer, IT:

1. Identify and remediate any desktops and laptops not currently managed in SCCM and/or Secunia.

2. Implement a process to ensure all corporate desktops and laptops are being managed in SCCM and Secunia.

3. Formally document the process used to manage Mac software patches in accordance with IT Standard Program and Process 12.004.

TVA Management's Comments – In response to our draft audit report, TVA management agreed with our findings and recommendations. See Appendix B for TVA management's complete response.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine the effectiveness of cyber security patching for high-risk, end-user desktops and laptops. Our scope was high-risk desktops and laptops managed by the Tennessee Valley Authority's (TVA) Information Technology (IT) on the corporate network. To achieve our objective, we:

1. Judgmentally selected a sample of 13 groups within TVA that we considered at high risk for spear phishing, based on their publicly known position or their access to sensitive TVA data.

   Of those 13 groups, we selected the full population of users in the following 8 groups based on their publicly known positions as well as their access to sensitive TVA data:

   - The Chief Executive Officer and direct reports (9 users)
   - The Senior Vice President and Chief Communications and Marketing Officer's direct reports (6 users)
   - The Executive Vice President of Generation and Chief Nuclear Officer's direct reports (8 users)
   - The Executive Vice President of Operations' direct reports (6 users)
   - The Executive Vice President and Chief External Relations Officer's direct reports (7 users)
   - The Senior Vice President and Chief Human Resources Officer's direct reports (7 users)
   - The Executive Vice President and General Counsel's direct reports (12 users)
   - The Executive Vice President and Chief Financial Officer's direct reports (10 users)

   For the remaining 5 groups we selected a nonstatistical random sample of users from each subgroup.[1] We selected these following groups based on their access to sensitive TVA data:

   - TVA IT System Administrators (10 of 39 users)
     - Server administrators (5 users)
     - Database administrators (5 users)
   - TVA Human Resources (19 of 41 users)
     - Employee Health (5 users)
     - Employee Benefits (5 users)

[1] For the nonstatistical random sample selections, we used a random number generator to select the users.

  - Equal Employment Opportunity (4 users)
  - Retirement (5 users)
- TVA Police Personnel Security (5 of 6 users)
- TVA Payroll (5 of 9 users)
- Office of General Counsel Legal Support Services (5 of 9 users)

In summary, we selected 109 users out of a total population from our selected groups of 169 users. Since this was a judgmental sample, the results of the sample cannot be projected to the population.

2. Obtained a listing of all users and their associated desktops and laptops using CAL, a system developed by TVA's IT. There were 162 computer desktops and laptops associated with the 109 users we selected.

3. Reviewed the patching status of Microsoft patches via access to a Web-based reporting tool for Microsoft's System Center Configuration Manager tool.

4. Reviewed the patching status of third-party (non-Microsoft) patches via access to a Web-based reporting tool for Flexera Software's Secunia (a tool that is used to deploy and report on third-party patches).

5. Reviewed any missing patches to determine if they could be used for remote code execution.

6. Reviewed any missing patches that could result in remote code execution to determine if there were publicly available exploits.

7. Followed up with TVA's IT management on any exceptions to determine if there was a business reason for those exceptions.

8. Reviewed IT Work Instruction 12.342, Windows Desktop Patch Management, and IT Standard Program and Process 12.004, Information Technology Patch and Vulnerability Management, to determine patch management documentation requirements.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require 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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

July 14, 2017

David P. Wheeler, ET 3C-K

RESPONSE TO REQUEST FOR COMMENTS – DRAFT AUDIT 2016-15369 - CYBER SECURITY PATCH MANAGEMENT OF HIGH-RISK DESKTOPS AND LAPTOPS

Our response to your request for comments regarding the findings of the subject draft report is attached. Please let us know if your staff has any concerns with TVA's comments.

We would like to thank Scott Marler, Michael Anderson, and the audit team for their professionalism and cooperation in conducting this audit. If you have any questions, please contact Krystal Brandenburg at (423) 751-6039.

Scott D. Self
Chief Information Officer
Information Technology
SP 3A-C

cc (Attachment):
Andrea S. Brackett, WT 5D-K
Krystal R. Brandenburg, MP 3C-C
Patrick Y. Buchanan, WT 9B-K
Clay Deloach, Jr., SP 3L-C
Robertson D. Dickens, WT 9C-K
Jeremy P. Fisher, MR 6D-C
Dwain K. Lanier, MR 3K-C
Philip D. Propes, MP 2B-C
Douglas E. Roelofs, MP 3B-C
Anthony M. Smith, MP 2H-C
Mark G. Spivey, MP 5C-C
John M. Thomas III, MR 6D-C
OIG File No. 2016-15369

DRAFT AUDIT 2016-15369
Cyber Security Patch Management of High-Risk Desktops and Laptops
Response to Request for Comments

ATTACHMENT A
Page 1 of 1

	Recommendation	Comments
1	Identify and remediate any desktops and laptops not currently managed in SCCM and/or Secunia.	Management agrees.
2	Implement a process to ensure all corporate desktops and laptops are being managed in SCCM and Secunia.	Management agrees.
3	Formally document the process used to manage Mac software patches in accordance with IT Standard Program and Process 12.004.	Management agrees.