Memorandum from the Office of the Inspector General

July 3, 2023

Gregory J. Henrich

FINAL REPORT – AUDIT 2022-17380 – TRANSMISSION AND POWER SUPPLY'S MANAGEMENT OF MAC® DESKTOPS AND LAPTOPS

As part of our annual audit plan, we audited the Tennessee Valley Authority (TVA) Transmission Operations and Power Supply[1] (TOPS) organization's management of Mac® desktops and laptops. Our objective was to determine if Mac® desktop and laptop patching and configuration management followed TVA policy. Patch management is the act of applying a change to installed software that corrects security or functionality problems. Configuration management is critical because it has a direct impact on the security posture of an information system.

In summary, we determined MacBooks® managed by TOPS followed TVA's configuration management policy. However, we determined 3 of 15 MacBooks® did not follow TVA policy for patch management. Specifically, one MacBook® was obsolete, and two had inconsistent patching history. In addition, we identified a gap between TVA policy and a TOPS patch management work instruction. Specifics of the findings and the corresponding devices have been omitted from this report due to their sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA management in a briefing on February 8, 2023.

As a result of our audit, TVA took action to (1) surplus one MacBook® we identified as obsolete and (2) update the TOPS work instruction to align with TVA policy.

In response to our draft report, TVA management agreed with the findings in the report. See the Appendix for TVA management's complete response.

BACKGROUND

The National Institute of Science and Technology (NIST) states:

> Software used for computing technologies must be maintained because there are many in the world who continuously search for and exploit flaws in software. Software maintenance includes patching, which is the act of applying a change to installed software – such as firmware, operating

[1] Transmission Operations and Power Supply is a group within the Transmission and Power Supply organization.

> systems, or applications – that corrects security or functionality problems or adds new capabilities. . . . Patch management is the process of identifying, prioritizing, acquiring, installing, and verifying the installation of patches, updates, and upgrades throughout an organization.[2]
>
> The configuration of a system and its components has a direct impact on the security posture of the system. . . . Effective configuration management is vital to the establishment and maintenance of security of information and systems. The security-focused configuration management process is critical to maintaining a secure state under normal operations, contingency recovery operations, and reconstitution to normal operations.[3]

The Cybersecurity and Infrastructure Security Agency (CISA) issued Binding Operational Directive 22-01, "Reducing the Significant Risk of Known Exploited Vulnerabilities" (KEVs) on November 3, 2021. This directive requires all federal civilian executive branch agencies to remediate KEVs within prescribed timeframes. The goal is to prioritize remediation efforts on the subset of vulnerabilities that adversaries are using to cause immediate harm.

In 2020, we audited the patching and configuration management of Mac® desktops and laptops managed by TVA's Technology and Innovation (T&I) organization.[4] We made three recommendations to T&I to address inventory inaccuracies, patching timeliness, and baseline configurations. In addition, we identified a population of Mac® devices that were not managed by TVA T&I but instead were managed by TVA's Transmission and Power Supply organization.

Within TVA's Transmission and Power Supply organization, the TOPS group oversees real-time operation of the transmission and generation resources under its control. TOPS is responsible for patch and configuration management of MacBooks® that are assigned to information system support personnel within their group. T&I manages most desktops and laptops within TVA; however, due to the real-time operation requirements, a population of 17 MacBooks® were in use by the TOPS group. One of these 17 MacBooks® were being managed by T&I, resulting in an initial population of 16 devices in scope for this audit.

As part of our annual audit planning, we completed a threat assessment to identify high-risk cybersecurity threats that could potentially impact TVA. We determined the potential impact for system intrusion through misconfigurations or unpatched systems to be high. Therefore, we included an audit of TVA TOPS management of Mac® desktops and laptops as part of our 2022 audit plan.

---

2 Murugiah Souppaya and Karen Scarfone, "Guide to Enterprise Patch Management Technologies," *NIST Special Publication 800-40,* Revision 4, April 2022, page iv, < https://doi.org/10.6028/NIST.SP.800-40r4 >, accessed on March 31, 2023.

3 Arnold Johnson, Dennis Bailey, Kelley Dempsey, Sarbari Gupta, Ron Ross "Guide for Security-Focused Configuration Management of Information Systems", *NIST Special Publication 800-128,* August 2011, page 6, < https://doi.org/10.6028/NIST.SP.800-128 >, accessed on March 31, 2023.

4 Audit Report 2020-15717, *Management of Mac® Desktops and Laptops*, August 20, 2020.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine if Mac® desktop and laptop patching and configuration management follow TVA policy. The scope of this audit was limited to Mac® desktops and laptops managed by TVA Transmission and Power Supply as of October 2022. Our fieldwork was conducted between September 2022 and March 2023. To achieve our objective, we:

- Obtained and reviewed the following Standard Programs and Processes (SPP):
  - TVA-SPP-12.004 – *TVA Cybersecurity Vulnerability Management Program.*
  - TVA-SPP-12.08.07 – *TVA Cybersecurity Classification of Computers.*
  - TVA-SPP-12.204 – *Internal Network Access Management for End User Devices.*
  - TVA-SPP-12.401 – *IT [Information Technology] Asset Procurement.*
  - TVA-SPP-12.704 – *Security Configuration Benchmark Standards.*
  - TVA-SPP-12.806 – *TVA Cybersecurity Patch and Remediation Management Program.*
- Reviewed TOPS *MacBook Requirements* (Work Instruction).
- Interviewed TOPS personnel and performed process walkthroughs to identify information on controls for management of Mac® desktops and laptops.
- Compared macOS® version installation dates against vendor patch release dates for 15 MacBooks® in use and managed by TOPS for a one year period. (Note: Although TOPS had 16 MacBooks® in use at the beginning of our audit, they subsequently determined one was obsolete and sent to T&I for surplus processing. Therefore, we did not include the obsolete device in our testing.)
- Reviewed macOS® version install dates against the CISA KEV catalog's publication dates for 15 MacBooks®.
- Reviewed TOPS work instruction for patch and configuration management and compared it against TVA's policy.

Vulnerability remediation and configuration management were identified as internal controls that were significant to our audit objective. 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 objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

FINDINGS

We determined all 15 MacBooks® managed by TOPS followed TVA configuration management policy. However, we determined 3 of the 15 MacBooks® did not follow TVA policy for patch management. Specifically, one MacBook® was obsolete, and two had inconsistent patching history. In addition, we identified a gap between TVA policy and a TOPS patch management work instruction.

INCONSISTENT PATCH HISTORY

We obtained the patch history of the 15 MacBooks® managed by TOPS and compared them to TVA policy requirements. Of those 15 MacBooks®, we determined one was considered obsolete by the vendor and no longer able to receive security patches or hardware support. Additionally, two of the 15 MacBooks® had inconsistently installed patches, the majority of which were installed over 14 days after their release. Although the patching for these two MacBooks® was current at the time of our testing, historically they had been vulnerable to KEVs outside of TVA policy's allowed remediation timeframe. As a result of our audit, TOPS sent the additional obsolete MacBook® to TVA T&I for surplus processing.

Specifics of the findings and the corresponding devices have been omitted from this report due to their sensitive nature in relation to TVA's cybersecurity but were formally communicated to TVA management in a briefing on February 8, 2023.

GAP BETWEEN TVA POLICY AND TOPS WORK INSTRUCTION

Our comparison of TVA-SPP-12.806, *TVA Cybersecurity Patch and Remediation Management Program*, and TVA-SPP-12.704, *Security Configuration Benchmark Standards*, to the TOPS work instruction for the management of MacBooks® found the TOPS patch management work instruction did not include steps to monitor the CISA KEVs catalog as required by TVA policy. As a result of our audit, TOPS updated their work instruction to include steps to monitor the CISA KEVs.

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

\- - - - - -

This report is for your review and information. No response to this report is necessary.

If you have any questions or need additional information please contact Andrew J. Jurbergs, Senior Auditor, at (865) 633-7393 or Sarah E. Huffman, Director, Information Technology Audits, at (865) 633-7345. We appreciate the courtesy and cooperation received from your staff during the audit.

David P. Wheeler
Assistant Inspector General
(Audits and Evaluations)

AJJ:KDS
cc: See page 5

cc: TVA Board of Directors
Mary C. Corbitt
Samuel P. Delk
Buddy Eller
David B. Fountain
James Patrick Hall
Jeffrey J. Lyash
Jill M. Matthews
Aaron P. Melda
Donald A. Moul
Ronald R. Sanders II
Ben R. Wagner
Kay W. Whittenburg
OIG File No. 2022-17380

June 28, 2023

David P. Wheeler, WT 2C-K

RESPONSE: DRAFT AUDIT 2022-17380 – Transmission and Power Supply's Management of Mac® Desktops and Laptops

Reference: OIG Memorandum dated June 6, 2023

Thank you for the opportunity to address the DRAFT Report for Evaluation 2022-17380 – Transmission and Power Supply's Management of Mac® Desktops and Laptops. We would like to thank Andrew Jurbergs and his team, for their professionalism and cooperation during this audit.

General Comments:
After review, we agree with the report and findings.

Greg Henrich
Vice President
Transmission Operations & Power Supply

GJH:ALC
cc: Mary C. Corbitt, MR 3K-C
Samuel P. Delk, BR 5A-C
David B. Fountain, WT 6A-K
J. Patrick Hall, MR 5E-C
Aaron P. Melda, MR 3H-C
Ronald R. Sanders II, MR 5E-C
Kay W. Whittenburg, MR 3A-C
OIG File No: 2022-17380