Office of the Auditor General
Follow-Up Report on Prior Audit Recommendations

Statewide UNIX Security Controls

Department of Technology, Management, and Budget

March 2024

State of Michigan Auditor General
Doug A. Ringler, CPA, CIA

171-0563-15F

The auditor general shall conduct post audits of financial transactions and accounts of the state and of all branches, departments, offices, boards, commissions, agencies, authorities and institutions of the state established by this constitution or by law, and performance post audits thereof.

The auditor general may make investigations pertinent to the conduct of audits.

Article IV, Section 53 of the Michigan Constitution

OAG
Office of the Auditor General

Report Summary

Follow-Up Report

Statewide UNIX Security Controls

Department of Technology, Management, and Budget (DTMB)

Report Number:
171-0563-15F

Released:
March 2024

We conducted this follow-up to determine whether DTMB took appropriate corrective measures in response to the two material conditions and one of the reportable conditions noted in our December 2015 audit report.

Prior Audit Information	Follow-Up Results		
	Conclusion	Finding	Agency Preliminary Response
Finding 1 - Material condition Improved security configuration controls needed to protect UNIX operating systems. Agency agreed.	Partially complied	Reportable condition exists. See Finding 1.	Agrees
Finding 2 - Reportable condition Establishment of approved UNIX operating system versions needed to protect confidential and critical information. Agency agreed.	Complied	Not applicable.	
Finding 5 - Material condition Enhancements to procedures for detecting and remediating security vulnerabilities are necessary. Agency agreed.	Substantially complied	Not applicable.	

Obtain Audit Reports

Online: audgen.michigan.gov

Phone: (517) 334-8050

Office of the Auditor General
201 N. Washington Square, Sixth Floor
Lansing, Michigan 48913

Doug A. Ringler, CPA, CIA
Auditor General

Laura J. Hirst, CPA
Deputy Auditor General

OAG
Office of the Auditor General

Doug A. Ringler, CPA, CIA
Auditor General

201 N. Washington Square, Sixth Floor • Lansing, Michigan 48913 • Phone: (517) 334-8050 • audgen.michigan.gov

March 21, 2024

Michelle Lange, Director
Department of Technology, Management, and Budget
and
Laura Clark, Chief Information Officer
Department of Technology, Management, and Budget
Elliott-Larsen Building
Lansing, Michigan

Director Lange and Chief Information Officer Clark:

This is our follow-up report on the two material conditions (Findings 1 and 5) and one of the reportable conditions (Finding 2). Within the scope of this follow-up, we included the corresponding recommendations for both Findings 1 and 2 and the first corresponding recommendation for Finding 5. We reported these findings and corresponding recommendations in our performance audit of Statewide UNIX Security Controls, Department of Technology, Management, and Budget. That audit report was issued and distributed in December 2015. Additional copies are available on request or at audgen.michigan.gov.

Your agency provided the preliminary response to the follow-up recommendation included in this report. The *Michigan Compiled Laws* and administrative procedures require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

We appreciate the courtesy and cooperation extended to us during our follow-up. If you have any questions, please call me or Laura J. Hirst, CPA, Deputy Auditor General.

Sincerely,

Doug Ringler

Doug Ringler
Auditor General

This Page Left Intentionally Blank

TABLE OF CONTENTS

STATEWIDE UNIX SECURITY CONTROLS

INTRODUCTION, PURPOSE OF FOLLOW-UP, AND AGENCY DESCRIPTION

INTRODUCTION

This report contains the results of our follow-up of the two material conditions* (Findings 1 and 5) and one of the reportable conditions* (Finding 2). Within the scope of this follow-up, we included the corresponding recommendations for both Findings 1 and 2 and the first corresponding recommendation for Finding 5. We reported these findings and corresponding recommendations in our performance audit* of Statewide UNIX Security Controls, Department of Technology, Management, and Budget (DTMB), issued in December 2015.

PURPOSE OF FOLLOW-UP

To determine whether DTMB had taken appropriate corrective measures to address our corresponding recommendations.

AGENCY DESCRIPTION

DTMB maintains and operates 13 identifiable variations of UNIX operating systems* on 884 UNIX servers. Systems and data critical for the operation and oversight of State government reside on these servers including systems for:

- Processing services and payments to citizens in need.
- Tracking and managing road and bridge construction projects and payments.
- Maintaining prisoner, parolee, and probation information.
- Processing the State employee payroll.

UNIX servers also provide a variety of enterprisewide functions, such as web, file, and print services; e-mail; patch* management; and virus protection as well as the software that stores, organizes, and provides access to systems.

** See glossary at end of report for definition.*

PRIOR AUDIT FINDINGS AND RECOMMENDATIONS; AGENCY PLAN TO COMPLY; AND FOLLOW-UP CONCLUSIONS, RECOMMENDATION, AND AGENCY PRELIMINARY RESPONSE

FINDING 1

Audit Finding Classification: Material condition.

Summary of the December 2015 Finding:
DTMB did not establish and implement effective operating system security* configuration* controls for the State's UNIX server environment. Specifically, we noted DTMB's UNIX servers had potentially vulnerable security configurations.

Recommendation Reported in December 2015:
We recommended DTMB establish and implement effective operating system security configuration controls for the State's UNIX server environment.

AGENCY PLAN TO COMPLY*

On March 7, 2016, DTMB stated it would:

- Improve operating system security configuration controls over the State's UNIX server environment. Specifically, DTMB indicated it had purchased the necessary automation tools and had initiated a project to enforce and maintain effective standardized operating system security configuration controls.
- Fully comply by June 2017.

FOLLOW-UP CONCLUSION

Partially complied. A reportable condition exists.

We randomly selected 40 of the State's 884 UNIX servers to review operating system security configurations and noted:

- 37 (93%) of 40 servers had potentially vulnerable security configurations. DTMB informed us it tailors configurations as part of the application installation process for a new server. However, these tailored configurations are not formally documented and, therefore, we were unable to determine if these configurations were potential security risks or approved tailored configurations.

  Because of the confidentiality* of these configurations, we summarized our testing results for presentation in this follow-up conclusion and provided the detailed results to DTMB management.

** See glossary at end of report for definition.*

- We could not review the security configurations for 3 of the 40 servers because they were running a documented but unsupported operating system version.

DTMB has made efforts to tailor UNIX server security configurations. DTMB implemented build configuration standards for hardening the operating system builds to industry best practice configuration benchmarks. However, these build configurations are only for blank UNIX servers. After the server is operational, DTMB tailors the configurations to ensure the application will function appropriately. DTMB does not always document the final configurations for these operational servers.

State of Michigan (SOM) Technical Standard 1340.00.060.01, which aligns with the National Institute of Standards and Technology* (NIST), states agency information system owners will establish and document configuration settings for components employed within the system (which includes servers and operating systems, according to NIST) that reflect the most restrictive mode consistent with operational requirements.

FOLLOW-UP RECOMMENDATION

We recommend DTMB document the establishment and implementation of effective operating system security configuration controls for the State's UNIX server environment.

FOLLOW-UP AGENCY PRELIMINARY RESPONSE

DTMB provided us with the following response:

DTMB agrees with the recommendation.

DTMB agrees with the importance of effective Operating System configuration controls. DTMB also agrees with the need to document tailored configuration settings.

DTMB acknowledges it did not always document the final configuration settings for the operational servers and the existing reporting tool did not always operate as intended.

DTMB will continue to update documentation associated with the tailored configuration settings.

** See glossary at end of report for definition.*

FINDING 2

Audit Finding Classification: Reportable condition.

Summary of the December 2015 Finding:
DTMB should establish a strategy to ensure only supported UNIX operating system versions are installed on servers. UNIX operating systems no longer supported by the vendor do not receive critical patches to address vulnerabilities*, which increases the risk to availability*, confidentiality, and integrity* of data residing within the State's applications. On average, operating system versions were unsupported for 7.2 years, with 5 versions being unsupported for over 10 years.

Recommendation Reported in December 2015:
We recommended DTMB establish a strategy to ensure only supported UNIX operating system versions are installed on servers containing the State's applications.

AGENCY PLAN TO COMPLY

On March 7, 2016, DTMB stated it would:

- Establish a strategy to ensure only supported UNIX operating system versions are installed on servers containing the State's applications.
- Utilize the Enterprise Architecture Roadmap to identify authorized and supported operating systems. DTMB has already begun issuing owners of unauthorized and unsupported operating systems a "Notice of Non-Compliance" and is working with the responsible departments to replace these systems.
- Ensure new operating system installations comply with the Enterprise Architecture Roadmap. In addition, DTMB is implementing a new IT infrastructure, the Next Generation Digital Infrastructure (NGDI), which will define acceptable UNIX operating systems and require State executive branch departments transitioning to the NGDI to use these operating systems.
- Fully comply by December 2016.

FOLLOW-UP CONCLUSION

Complied.

Our review of DTMB's Configuration Management Database (CMDB) noted 3 (23%) of the 13 identifiable UNIX operating system versions were unsupported and operating on 20 (2%) of the State's 878 UNIX servers. DTMB documented its approval for utilizing unsupported operating systems on these servers.

** See glossary at end of report for definition.*

FINDING 5

Audit Finding Classification: Material condition.

Summary of the December 2015 Finding:
DTMB did not fully establish and implement effective procedures to detect and remediate security vulnerabilities.

Our review of DTMB's process to detect and remediate UNIX server vulnerabilities disclosed:

a. Vulnerability scans, using the State's current vulnerability management tool, did not detect whether critical configuration settings were implemented.

b. Vulnerability scans were not performed monthly on all UNIX servers. Therefore, DTMB did not remediate vulnerabilities in a timely manner.

c. Security baseline configurations* were not fully established by DTMB. We noted:

   (1) DTMB did not adopt a UNIX security configuration checklist.

   (2) Hardening* procedures, designed to ensure appropriate server security is in place before a server is deployed in the production environment, were not established for two UNIX versions. Also, three procedures did not meet industry best practice recommendations for certain configuration settings.

d. The server automation tool purchased by DTMB to help detect operating system vulnerabilities was not installed on all servers.

Recommendation Reported in December 2015:
We recommended DTMB fully establish and implement effective procedures to detect and remediate security vulnerabilities on UNIX servers.

AGENCY PLAN TO COMPLY

On March 7, 2016, DTMB indicated it:

- Purchased the necessary automation tools and initiated a project to install the tools on all UNIX servers. The new tools will automate the detection and remediation of security vulnerabilities.

- Is developing a process to assign responsibilities, between Technical Services, Agency Services, and Network and Telecommunication Division, for the remediation of threats* detected in vulnerability scans.

** See glossary at end of report for definition.*

- Will utilize existing server management standards, new vulnerability scan procedures, new monitoring processes, and new operational compliance reports to enhance the detection and remediation of security vulnerabilities. All procedures will be reviewed at least annually to meet industry best practices.

- Will fully comply by June 2017.

FOLLOW-UP CONCLUSION

Substantially complied.

Our review of DTMB's process to detect and remediate UNIX server vulnerabilities disclosed DTMB:

a. Complied.

   DTMB's monitoring tool scans servers to detect whether critical configuration settings are not implemented. Examples of critical security configurations detected by the scans include password configurations, log-in configurations, file permissions, and user account configuration management. We reviewed the scan results for our follow-up for Finding 1.

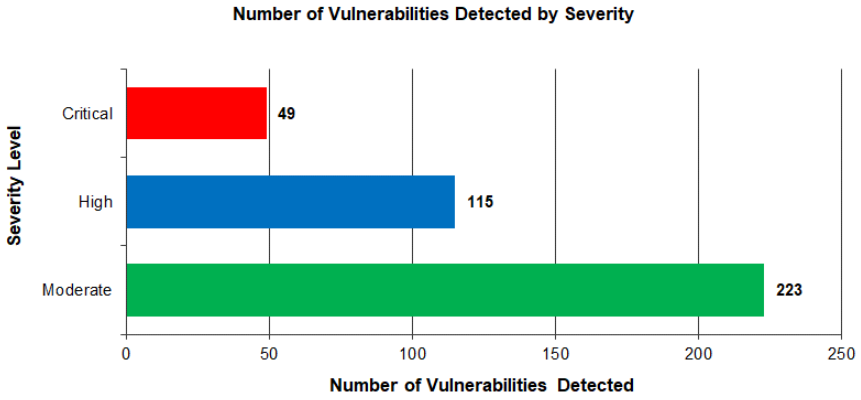
b. Partially complied.

   We randomly sampled and tested 40 UNIX servers and noted:

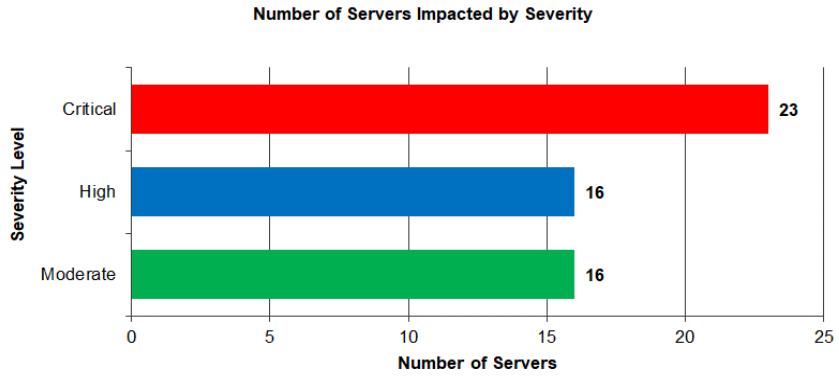
   (1) All servers were scanned at least once per month.

   (2) Vulnerabilities existed on 28 (70%) of the 40 servers which DTMB had not remediated in a timely manner. However, we noted a 92% decrease in the total number of outstanding vulnerabilities since our December 2015 report.

(3) The following charts summarize the number of vulnerabilities detected and number of servers impacted for severity levels moderate through critical:



Source: The OAG created this chart using data from testing results of DTMB's vulnerability remediation.



Source: The OAG created this chart using data from testing results of DTMB's vulnerability remediation.

c. Substantially complied.

DTMB did not implement baseline security configurations for operational and application loaded servers. We noted DTMB:

(1) Adopted UNIX security configuration checklists and established build configuration standards, which it used for hardening the operating system builds to industry best practice configuration benchmarks. NIST Special Publication 800-70 Revision 4 states that a security configuration checklist is a series of instructions or procedures for configuring an IT product to a particular operational environment, for verifying the product has been configured properly, and for identifying unauthorized changes to the product.

DTMB informed us that these build configurations are only for blank UNIX servers. After the server is operational, DTMB tailors the configurations to ensure the application will function appropriately. However, DTMB does not always document the final configurations for these operational servers. Therefore, there is not a documented baseline configuration for the operational and application loaded servers.

According to SOM Technical Standard 1345.00.13, DTMB will ensure that server builds are tailored from components of NIST Special Publication 800-53, the Center for Internet Security*, and SOM policies, standards, and procedures. SOM Technical Standard 1340.00.060.01, which aligns with NIST, states agency information system owners will establish and document configuration settings for components employed within the system (which includes servers and operating systems according to NIST) that reflect the most restrictive mode consistent with operational requirements.

(2) Established hardening guides which met industry best practice recommendations for the selected sample of operating system versions.

d. Complied.

DTMB installed the scanning tool on all servers and scanned all 40 sampled servers at least once per month.

** See glossary at end of report for definition.*

FOLLOW-UP METHODOLOGY, PERIOD, AND AGENCY RESPONSES

FOLLOW-UP METHODOLOGY

We reviewed DTMB's corrective action plan and updated technical standards related to UNIX servers. Specifically, for:

- Finding 1, we:
    - Met with DTMB staff to obtain an understanding of DTMB's procedures for hardening UNIX servers.
    - Reviewed data recorded in the CMDB to isolate a population of operational UNIX servers.
    - Pulled a sample of configurations to compare against DTMB's configuration monitoring report.
    - Obtained a copy of DTMB's configuration monitoring report and determined its reliability.
    - Pulled a random sample of 40 of 884 UNIX servers and compared server configurations with DTMB policies and industry best practices.
- Finding 2, we:
    - Met with DTMB staff to obtain an understanding of DTMB's procedures for identifying and removing servers with unsupported versions of UNIX operating systems.
    - Analyzed DTMB's 878 servers from the CMDB inventory to identify unsupported versions of UNIX operating systems. This count does not include 6 servers which were not in the CMDB inventory.
    - Reviewed DTMB documentation to support remediation of 6 unsupported operating system versions.
    - Reviewed approvals from the Technical Review Board allowing DTMB to continue utilizing unsupported operating system versions.
- Finding 5, we:
    - Interviewed DTMB management to obtain an understanding of DTMB's vulnerability patching process.
    - Obtained and reviewed DTMB vulnerability scans for 40 of 884 selected UNIX servers to

assess DTMB's processes for monitoring and remediating security vulnerabilities.

- Tested DTMB's policies, standards, and procedures against industry best practices.

PERIOD

Our follow-up generally covered July 12, 2023 through December 5, 2023.

AGENCY RESPONSES

Our follow-up report contains 1 recommendation. DTMB's preliminary response indicates it agrees with the recommendation.

The agency preliminary response following the follow-up recommendation in our report was taken from the agency's written comments and oral discussion at the end of our fieldwork. Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100) require an audited agency to develop a plan to comply with the recommendations and to submit it to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.

GLOSSARY OF ABBREVIATIONS AND TERMS

agency plan to comply	The response required by Section 18.1462 of the *Michigan Compiled Laws* and the State of Michigan Financial Management Guide (Part VII, Chapter 4, Section 100). The audited agency is required to develop a plan to comply with Office of the Auditor General audit recommendations and to submit the plan to the State Budget Office upon completion of an audit. Within 30 days of receipt, the Office of Internal Audit Services, State Budget Office, is required to review the plan and either accept the plan as final or contact the agency to take additional steps to finalize the plan.
availability	Timely and reliable access to data and information systems.
baseline configuration	A set of specifications for a system, or configuration item within a system, that has been formally reviewed and agreed on at a given point in time and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
Center for Internet Security	A not-for-profit organization that establishes and promotes the use of consensus-based best practice standards to raise the level of security and privacy in information technology systems.
CMDB	Configuration Management Database.
confidentiality	Protection of data from unauthorized disclosure.
configuration	The way a system is set up. Configuration can refer to either hardware or software or the combination of both.
database	A collection of information organized so it can be easily accessed, managed, and updated.
DTMB	Department of Technology, Management, and Budget.
hardening	Configuring an operating system and applications to reduce security weaknesses.
integrity	Accuracy, completeness, and timeliness of data in an information system.
IT	information technology.

material condition	A matter that, in the auditor's judgment, is more severe than a reportable condition and could impair the ability of management to operate a program in an effective and efficient manner and/or could adversely affect the judgment of an interested person concerning the effectiveness and efficiency of the program. Our assessment of materiality is in relation to the respective audit objective.
National Institute of Standards and Technology (NIST)	An agency of the Technology Administration, U.S. Department of Commerce. NIST's Computer Security Division develops standards, security metrics, and minimum security requirements for federal programs.
operating system	The essential program in a computer that manages all the other programs and maintains disk files, runs applications, and handles devices such as the mouse and printer.
patch	An update to an operating system, applications, or other software issued specifically to correct particular problems with the software.
performance audit	An audit that provides findings or conclusions based on an evaluation of sufficient, appropriate evidence against criteria. Performance audits provide objective analysis to assist management and those charged with governance and oversight in using the information to improve program performance and operations, reduce costs, facilitate decision-making by parties with responsibility to oversee or initiate corrective action, and contribute to public accountability.
reportable condition	A matter that, in the auditor's judgment, is less severe than a material condition and falls within any of the following categories: a deficiency in internal control; noncompliance with provisions of laws, regulations, contracts, or grant agreements; opportunities to improve programs and operations; or fraud.
security	Safeguarding an entity's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity.
SOM	State of Michigan.
threat	An activity, intentional or unintentional, with the potential for causing harm to an automated information system or activity.
vulnerability	Weakness in an information system that could be exploited or triggered by a threat.

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

This Page Left Intentionally Blank

Report Fraud/Waste/Abuse

Online: audgen.michigan.gov/report-fraud

Hotline: (517) 334-8070