STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
  Date: 09/05/2025
  STIG Finding: STIG ID: WN11-AU-000050
- **SRG:** SRG-OS-000064-GPOS-00033
  Severity: medium
  Vulnerability ID: V-253312 **CCI:** CCI-000172,CCI-003938

---

1. Introduction

This report documents the process of identifying, remediating, and verifying the fix for a Windows 11 STIG compliance finding. The selected finding was: STIG ID: WN11-AU-000050 “The system must be configured to audit Detailed Tracking - Process Creation successes.”

---

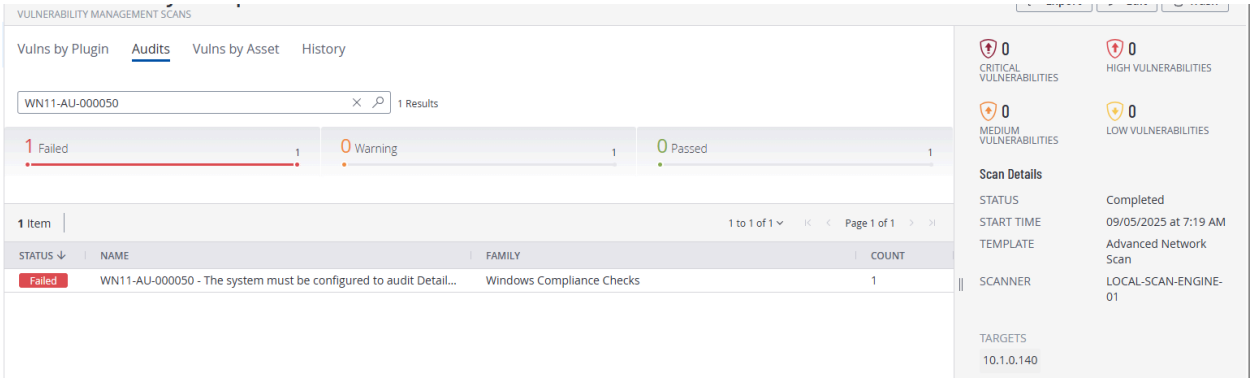
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-AU-000050
- Status: **Fail** (non-compliant)

📎 **Evidence:** First identified the STIG:

https://stigaview.com/products/win11/v2r1/WN11-AU-000050/

After initial scan results:



---

3. Manual Remediation Steps

Run "gpedit.msc".

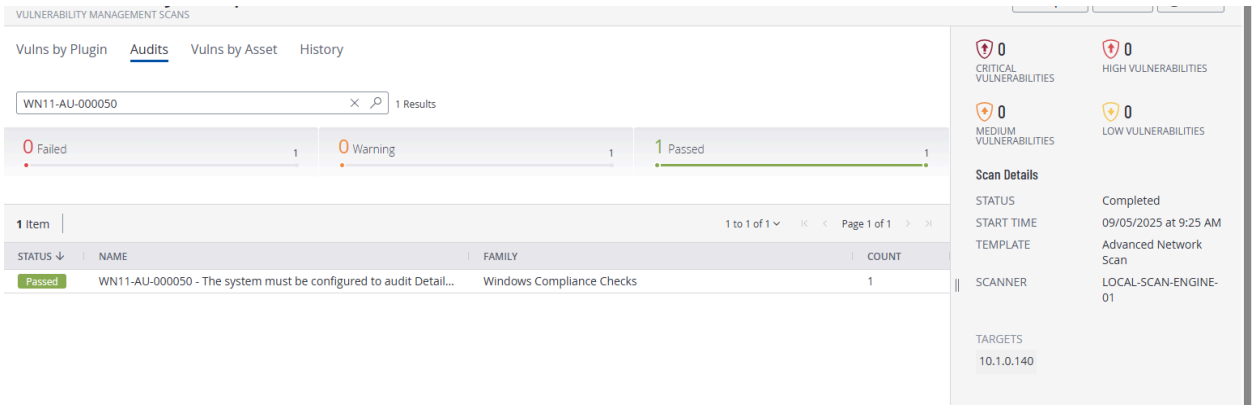
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Detailed Tracking >> "Audit Process Creation" with "Success" selected.

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-AU-000050
- Status: Passed

Evidence:



---

4. Reintroduction of Finding (Manually Undo Test)

To demonstrate full control of the setting, the fix was undone:

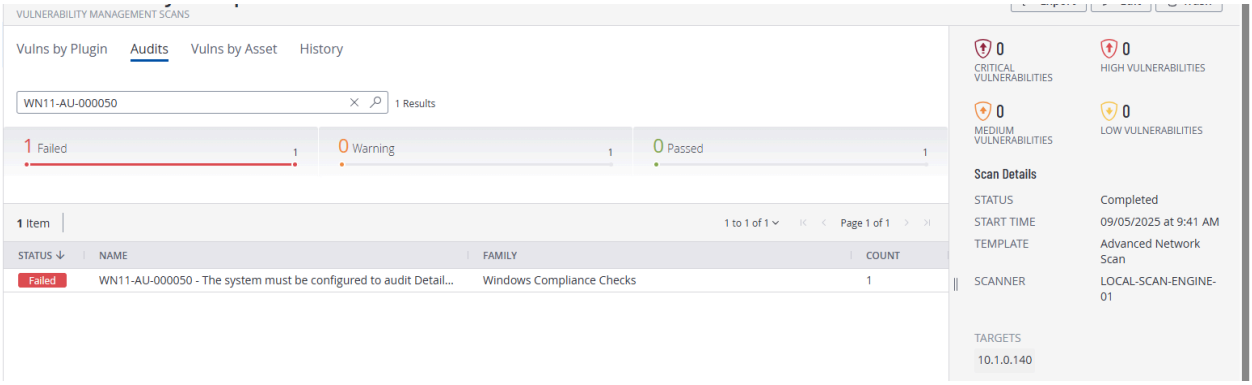
- Disabled the setting. Open **Group Policy Management** (`gpedit.msc`) and followed the instructions for remediation from before and set it to the original setting: Nothing Selected.

- Ran `gpupdate /force` and rescanned.
- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)

- Finding ID: WN11-AU-000050

Status: Failed, Non-Compliant

Evidence:



---

5. Remediation with PowerShell Script

Why a script will not reliably remediate WN11-AU-000050:

- This STIG controls **Advanced Audit Policy settings** (Audit Process Creation → Success).

- On Windows 11, these settings can be **enforced by Group Policy (domain or local)**.

- Running a PowerShell script with `auditpol.exe` **only changes the in-memory or local setting**, but:

- If a higher-level policy exists, it **overrides the script**,
- After a reboot or policy refresh, the change may be reverted.

- Therefore, the only reliable way to ensure compliance is to **manually configure the setting** in the Local Security Policy (or the controlling GPO).

Manual Remediation

Run "gpedit.msc".

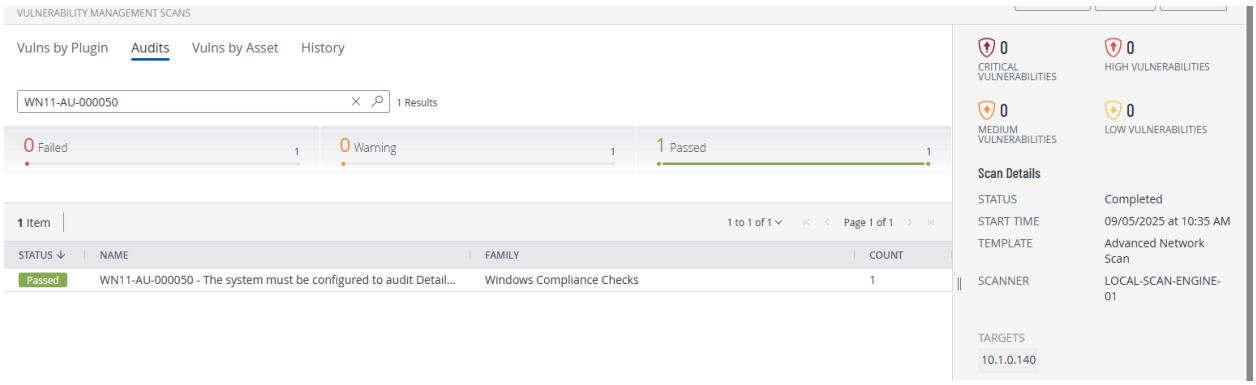
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Detailed Tracking >> "Audit Process Creation" with "Success" selected.

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-AU-000050
- Status: Passed

Evidence:



6. Conclusion

The finding **WN11-AU-000050** was successfully:

- Detected in an initial Tenable STIG Audit scan,
- Remediated manually,
- Verified through a second scan,
- Undone and confirmed as vulnerable again,
- Finally remediated manually and validated with a third scan.

This demonstrates the ability to manage Windows STIG compliance manually.