STIG Implementation Report

Intern Credit Application For: Bruce Thornton
Date: 09/06/2025
STIG Finding: STIG ID: WN11-AU-000560
SRG: SRG-OS-000037-GPOS-00015
Severity: Medium
Vulnerability ID: V-253345 **CCI:** CCI-000130

---

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: **WN11-AU-000560**, which requires that “Windows 11 must be configured to audit other Logon/Logoff Events Successes.”

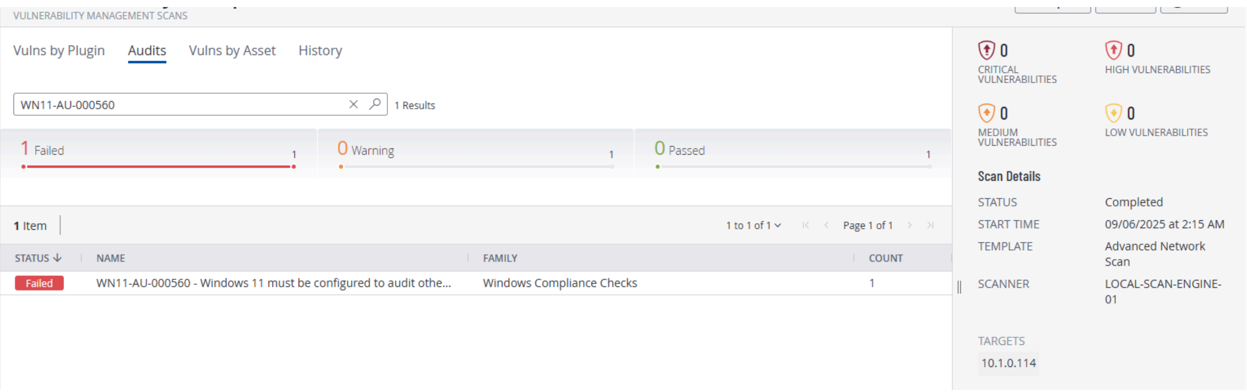
---

2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-AU-000560
- Status: **Fail** (non-compliant)

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

https://stigaview.com/products/win11/v1r5/WN11-AU-000560/



WN11-AU-000560 1 Results

1 Failed 1 | 0 Warning 1 | 0 Passed 1

1 Item | 1 to 1 of 1 | Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Failed	WN11-AU-000560 - Windows 11 must be configured to audit othe...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES
0 HIGH VULNERABILITIES
0 MEDIUM VULNERABILITIES
0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	09/06/2025 at 2:15 AM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.114

---

3. Manual Remediation Steps

Run "gpedit.msc".

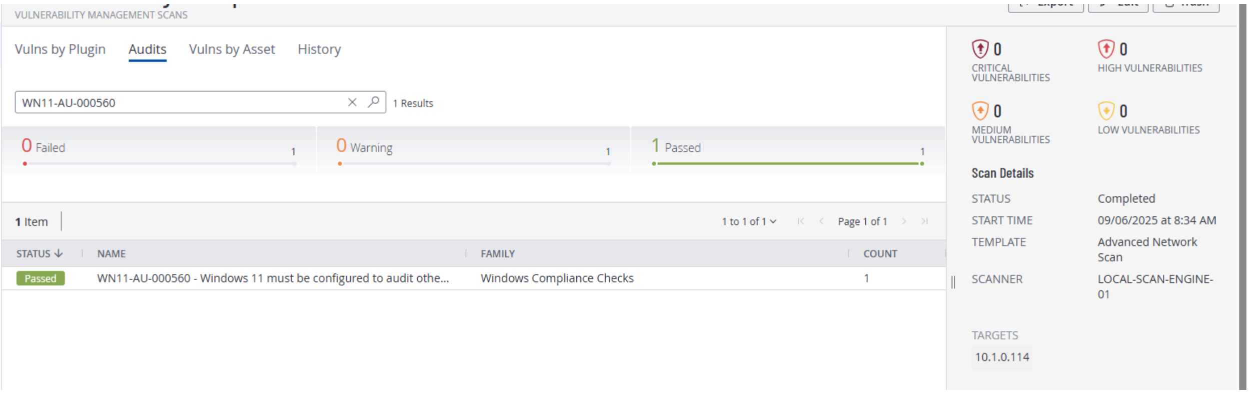
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> "Audit Other Logon/Logoff Events" with "Success" selected.

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-AU-000560
- Status: Passed

Evidence:



WN11-AU-000560 1 Results

0 Failed 1 | 0 Warning 1 | 1 Passed 1

1 Item | 1 to 1 of 1 | Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Passed	WN11-AU-000560 - Windows 11 must be configured to audit othe...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES | 0 HIGH VULNERABILITIES
0 MEDIUM VULNERABILITIES | 0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	09/06/2025 at 8:34 AM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.114

4. Reintroduction of Finding (Manually Undo Test)

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

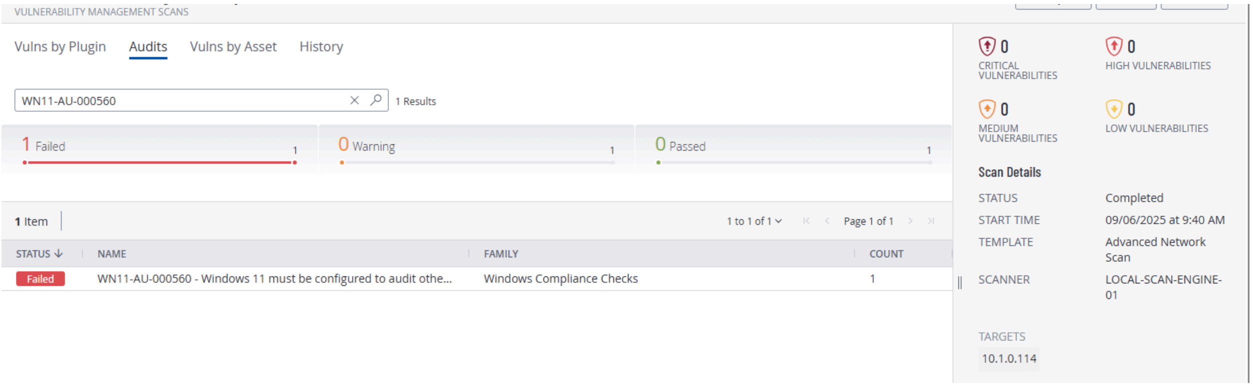
- Disabled the setting. Open **Group Policy Management** (`gpedit.msc`) and followed the instructions for remediation from before and set it to the original setting: Nothing Selected.

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

- Finding ID: WN11-AU-000050

Status: Failed, Non-Compliant

Evidence:



WN11-AU-000560 1 Results

1 Failed 1 | 0 Warning 1 | 0 Passed 1

1 Item | 1 to 1 of 1 | Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Failed	WN11-AU-000560 - Windows 11 must be configured to audit othe...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES | 0 HIGH VULNERABILITIES
0 MEDIUM VULNERABILITIES | 0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	09/06/2025 at 9:40 AM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.114

5. Remediation with PowerShell Script

For **STIG ID: WN11-AU-000560 (Audit Other Logon/Logoff Events – Success)**, multiple efforts were made to remediate the control using PowerShell scripts. Initial attempts utilized `auditpol.exe /set` to enable Success auditing for the "Other Logon/Logoff Events" subcategory and verify the configuration. A secondary approach attempted to use `auditpol.exe /restore` with a manually created CSV to make the change persistent, but this method failed due to invalid data formatting, as `auditpol /restore` only accepts backup files generated by `auditpol /backup`. After testing and verification, it was determined that the audit setting is controlled by Local Security Policy and/or Group Policy, causing any script-based changes to revert on reboot or policy refresh. Therefore, full remediation of this STIG can only be reliably performed manually through **gpedit.msc** → **Advanced Audit Policy Configuration** → **Logon/Logoff** → **Audit Other Logon/Logoff Events (Success)**.

Manual Remediation:

Run "gpedit.msc".

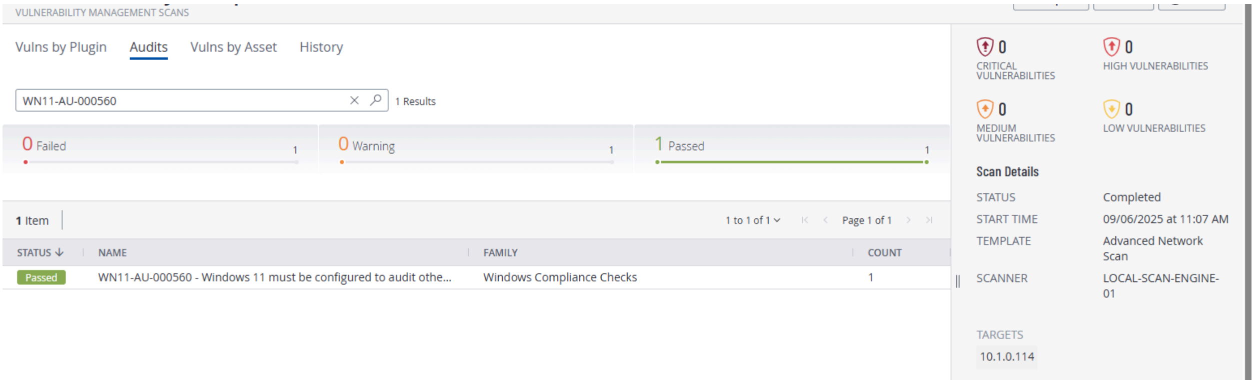
Configure the policy value for Computer Configuration >> Windows Settings >> Security Settings >> Advanced Audit Policy Configuration >> System Audit Policies >> Logon/Logoff >> "Audit Other Logon/Logoff Events" with "Success" selected.

Run "gpupdate /force" and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-AU-000560
- Status: Passed

Evidence:



WN11-AU-000560 1 Results

0 Failed 1

0 Warning 1

1 Passed 1

1 Item

1 to 1 of 1 Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Passed	WN11-AU-000560 - Windows 11 must be configured to audit othe...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES

0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES

0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	09/06/2025 at 11:07 AM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

10.1.0.114

6. Conclusion

The finding **WN11-AU-000560** was successfully:

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

This demonstrates the ability to manage Windows STIG compliance manually.