

STIG Implementation Report

Intern Credit Application For: Bruce Thornton

Date: 09/05/2025

STIG Finding: STIG ID: WN11-CC-000090

SRG: SRG-OS-000480-GPOS-00227

Severity: Medium


Vulnerability ID: V-253373

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-CC-000090**, which requires that Group Policy be configured to process registry policy settings even if Group Policy objects have not changed.

2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000090
- Status: **Fail** (non-compliant)

 **Evidence:** First identified the STIG:
<https://stigaview.com/products/win11/v2r1/WN11-CC-000090/>

Included with the initial scan:

VULNERABILITY MANAGEMENT SCANS			
Vulns by Plugin Audits Vulns by Asset History			
WN11-CC-000090 1 Results			
<div> <div>1 Failed</div> <div>0 Warning</div> <div>0 Passed</div> </div>			
1 Item <div>1 to 1 of 1</div> <div>Page 1 of 1</div>			
STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000090 - Group Policy objects must be reprocessed eve...	Windows Compliance Checks	1
<div> <div>0 CRITICAL VULNERABILITIES</div> <div>0 HIGH VULNERABILITIES</div> <div>0 MEDIUM VULNERABILITIES</div> <div>0 LOW VULNERABILITIES</div> </div> <div> <div>Scan Details</div> <div> <div>STATUS</div> <div>START TIME</div> <div>TEMPLATE</div> <div>SCANNER</div> <div>TARGETS</div> </div> <div> <div>Completed</div> <div>09/05/2025 at 9:49 PM</div> <div>Advanced Network Scan</div> <div>LOCAL-SCAN-ENGINE-01</div> <div>10.1.0.232</div> </div> </div>			

3. Manual Remediation Steps

Performed the following changes:

- Opened **Local Group Policy Editor** (`gpedit.msc`).
- Navigated to: `Computer Configuration` → `Administrative Templates` → `System` → `Group Policy`
- Enabled **Configure registry policy processing**.
- Selected “**Process even if the Group Policy objects have not changed.**”
- Ran `gpupdate /force` and rebooted the VM.

4. Verification Scan Results (After Fix)

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000090
- Status: Passed

Evidence:

VULNERABILITY MANAGEMENT SCANS			
Vulns by Plugin Audits Vulns by Asset History			
WN11-CC-000090 1 Results			
0 Failed 1 Warning 1 Passed			
1 Item 1 to 1 of 1 Page 1 of 1			
STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000090 - Group Policy objects must be reprocessed eve...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES

0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES

0 LOW VULNERABILITIES

Scan Details

STATUS Completed

START TIME 09/05/2025 at 10:04 PM

TEMPLATE Advanced Network Scan

SCANNER LOCAL-SCAN-ENGINE-01

TARGETS 10.1.0.232

5. Reintroduction of Finding (Undo Test)

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

- Disabled the setting in Local Group Policy Editor (or reverted registry value).
- Ran `gpupdate /force` and rescanned.
- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000090
- Status: Passed

Evidence:

VULNERABILITY MANAGEMENT SCANS			
Vulns by Plugin Audits Vulns by Asset History			
WN11-CC-000090 1 Results			
1 Failed 1 Warning 1 Passed			
1 Item 1 to 1 of 1 Page 1 of 1			
STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000090 - Group Policy objects must be reprocessed eve...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES

0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES

0 LOW VULNERABILITIES

Scan Details

STATUS Completed

START TIME 09/05/2025 at 10:16 PM

TEMPLATE Advanced Network Scan


SCANNER LOCAL-SCAN-ENGINE-01

TARGETS 10.1.0.232

6. Remediation

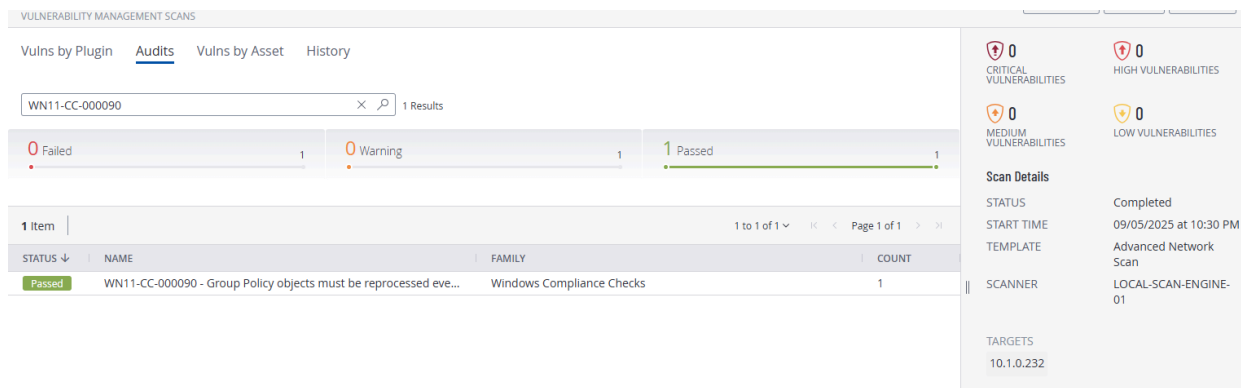
For **WN11-CC-000090** (“Configure registry policy processing”), the **only fully supported way to apply it is via Local Group Policy Editor (gpedit.msc) or a domain GPO.**

- Just creating a registry key/value manually (via PowerShell or regedit) **does not update the Group Policy setting in gpedit.**
- That’s why when you open **gpedit.msc**, it still says Not Configured, and the checkboxes are not selected.
- Tenable checks the **actual policy state**, not just whether a registry value exists, so a raw registry edit alone won’t make it compliant.
- gpupdate /force, must still be ran, along with restart/reboot.

 **Evidence:** Manual check showed that these changes were saved/enabled following the Manual directions from before.

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000090

Tenable Scan Results: **PASS**



The screenshot displays the Tenable Vulnerability Management Scans interface. The top navigation bar includes 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. The 'Audits' tab is selected, and a search filter 'WN11-CC-000090' is applied, resulting in '1 Results'. Below the search bar, a summary bar shows '0 Failed', '0 Warning', and '1 Passed'. The main table lists the audit results:

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000090 - Group Policy objects must be reprocessed eve...	Windows Compliance Checks	1

On the right side, the 'Scan Details' panel provides additional information:

- CRITICAL VULNERABILITIES:** 0
- HIGH VULNERABILITIES:** 0
- MEDIUM VULNERABILITIES:** 0
- LOW VULNERABILITIES:** 0
- STATUS:** Completed
- START TIME:** 09/05/2025 at 10:30 PM
- TEMPLATE:** Advanced Network Scan
- SCANNER:** LOCAL-SCAN-ENGINE-01
- TARGETS:** 10.1.0.232

7. Conclusion

The finding **WN11-CC-000090** 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.