STIG Implementation Report

Intern Credit Application For: Bruce Thornton
Date: 08/29-30/2025
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

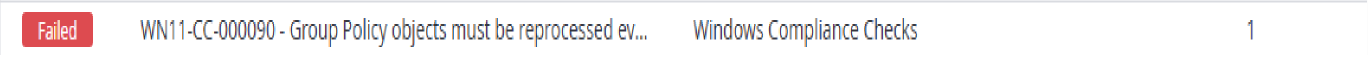
- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000090
- Status: **Fail** (non-compliant)

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

Included with the full Audit Only results:

WN11-CC-000090 - Group Policy objects must be reprocessed even if they have not changed. Info Enabling this setting and then selecting the 'Process even if the Group Policy objects have not changed' option ensures that the policies will be reprocessed even if none have been changed. This way, any unauthorized changes are forced to match the domain-based group policy settings again. Solution Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Group Policy >> 'Configure registry policy processing' to 'Enabled' and select the option 'Process even if the Group Policy objects have not changed'.

See Also
https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R3_STIG.zip
References 800-171 800-171R3 800-53 800-53R5 CAT CCI CN-L3 CSF CSF2.0 CSF2.0 DISA_BENCHMARK GDPR HIPAA ISO-27001-2022 ITSG-33 NESA RULE-ID STIG-ID SWIFT-CSCV1 VULN-ID Assets 10.1.0.45 3.4.2 03.04.02a. CM-6b. CM-6b. II CCI-000366 8.1.10.6(d) PR.IP-1 DE.CM-09 PR.PS-01 Microsoft_Windows_11_STIG 32.1.b 164.306(a)(1) A.8.9 CM-6b. T3.2.1 SV-253373r991589_rule WN11-CC-000090 2.3 V-253373 NULL



Failed	WN11-CC-000090 - Group Policy objects must be reprocessed ev...	Windows Compliance Checks	1

---

3. Manual Remediation Steps

Performed the following changes:

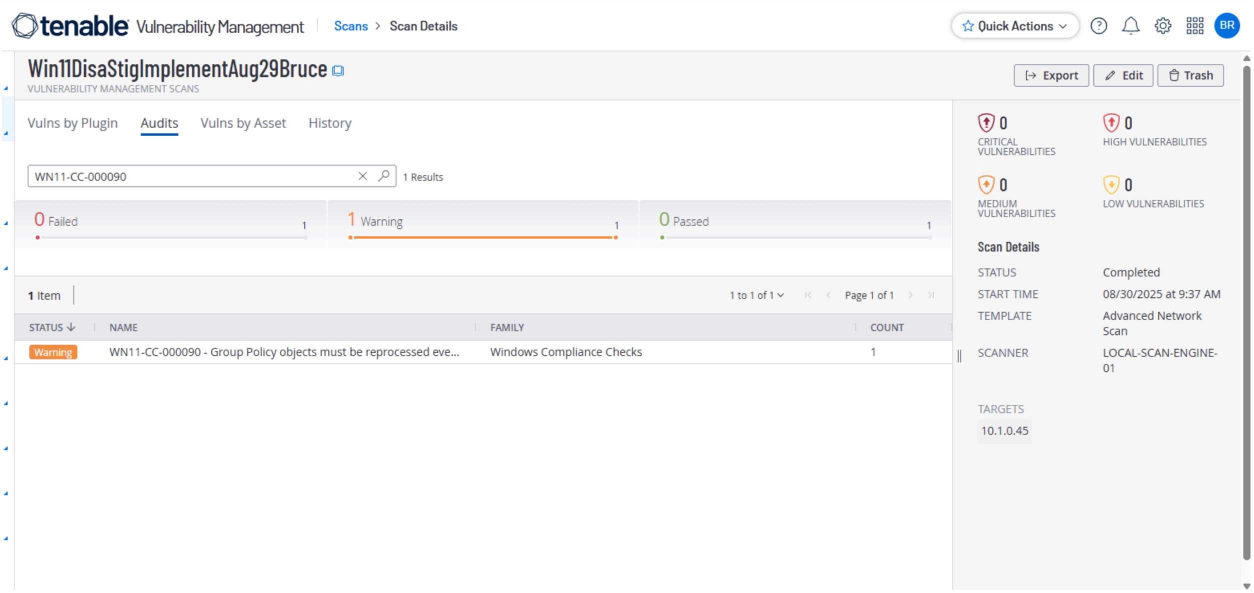
1. Opened **Local Group Policy Editor** (`gpedit.msc`).
2. Navigated to: `Computer Configuration → Administrative Templates → System → Group Policy`
3. Enabled **Configure registry policy processing**.
4. Selected **“Process even if the Group Policy objects have not changed.”**
5. Ran `gpupdate /force` 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: Warning/**Pass** (compliant, neither pass nor fail)

📎 **Evidence:**



Win11DisaStigImplementAug29Bruce

VULNERABILITY MANAGEMENT SCANS

WN11-CC-000090 — 1 Results

0 Failed 1 | 1 Warning 1 | 0 Passed 1

1 Item — 1 to 1 of 1 — Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Warning	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	08/30/2025 at 9:37 AM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

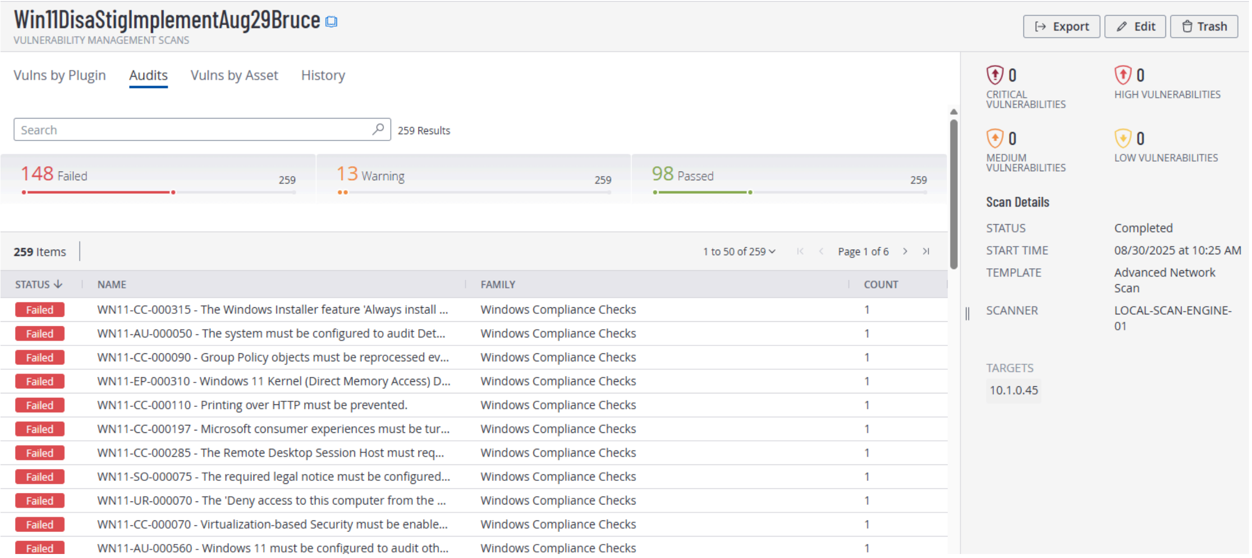
10.1.0.45

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.

📎 **Evidence:**



Win11DisaStigImplementAug29Bruce

VULNERABILITY MANAGEMENT SCANS

259 Results

148 Failed 259 | 13 Warning 259 | 98 Passed 259

259 Items — 1 to 50 of 259 — Page 1 of 6

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000315 - The Windows Installer feature 'Always install ...	Windows Compliance Checks	1
Failed	WN11-AU-000050 - The system must be configured to audit Det...	Windows Compliance Checks	1
Failed	WN11-CC-000090 - Group Policy objects must be reprocessed ev...	Windows Compliance Checks	1
Failed	WN11-EP-000310 - Windows 11 Kernel (Direct Memory Access) D...	Windows Compliance Checks	1
Failed	WN11-CC-000110 - Printing over HTTP must be prevented.	Windows Compliance Checks	1
Failed	WN11-CC-000197 - Microsoft consumer experiences must be tur...	Windows Compliance Checks	1
Failed	WN11-CC-000285 - The Remote Desktop Session Host must req...	Windows Compliance Checks	1
Failed	WN11-SO-000075 - The required legal notice must be configured...	Windows Compliance Checks	1
Failed	WN11-UR-000070 - The 'Deny access to this computer from the ...	Windows Compliance Checks	1
Failed	WN11-CC-000070 - Virtualization-based Security must be enable...	Windows Compliance Checks	1
Failed	WN11-AU-000560 - Windows 11 must be configured to audit oth...	Windows Compliance Checks	1

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

Scan Details

STATUS	Completed
START TIME	08/30/2025 at 10:25 AM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

10.1.0.45

6. Remediation

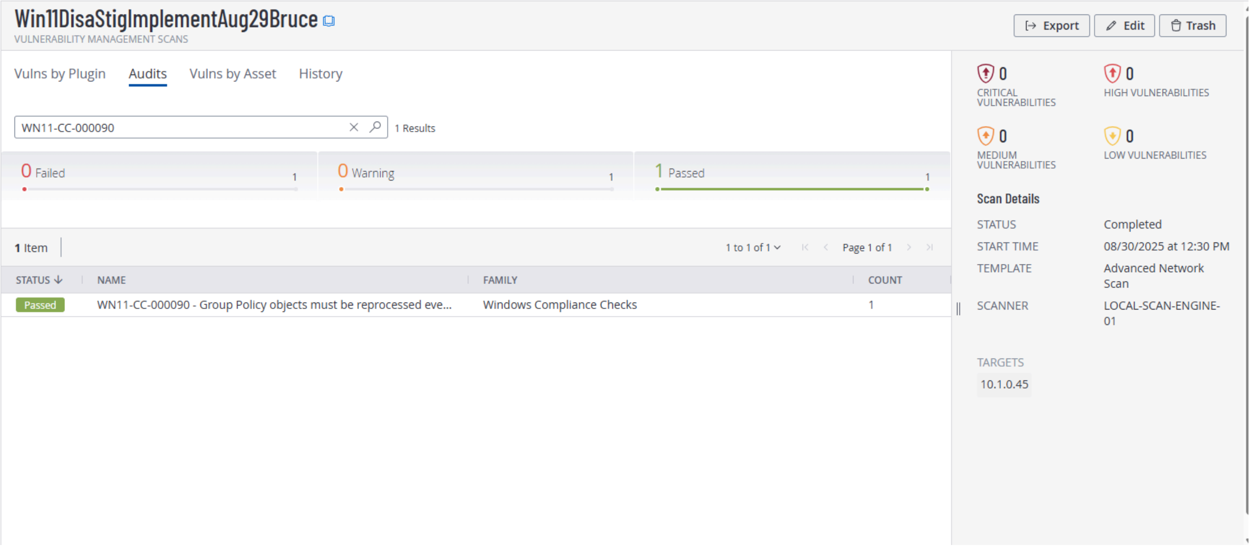
For **WN11-CC-000090** (“Configure registry policy processing”), the **only fully supported way to apply it is via Local Group Policy Editor (gpedit.msc) or a domain GPO**.

- 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 directions from before.

Tenable Scan Results: **PASS**



Win11DisaStigImplementAug29Bruce

VULNERABILITY MANAGEMENT SCANS

WN11-CC-000090 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-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	08/30/2025 at 12:30 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

10.1.0.45

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.