

STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
Date: 09/07/2025
STIG Finding: STIG ID: WN11-CC-000310
 - **SRG:** [SRG-OS-000362-GPOS-00149](#)
Severity: medium
Vulnerability ID: V-253410 **CCI:** CCI-003980
-

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-CC-000310 "Users must be prevented from changing installation options."

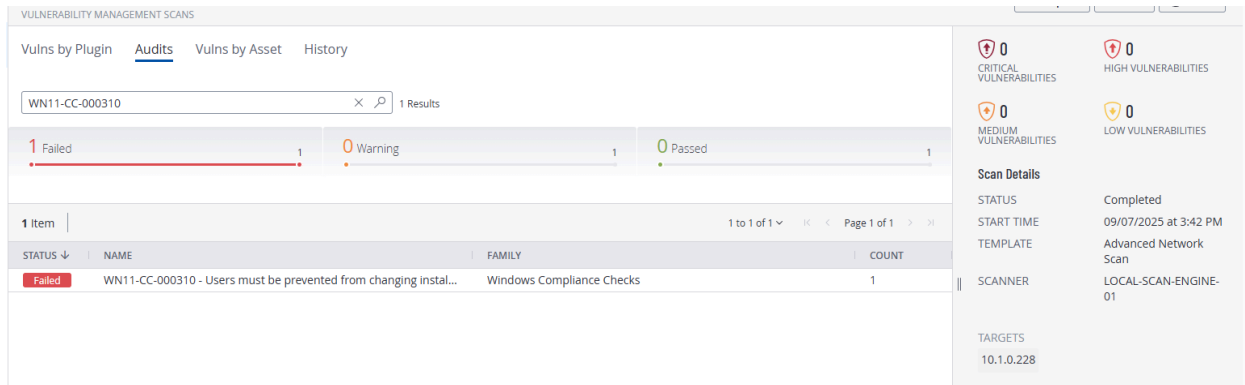
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000310
- Status: **Fail** (non-compliant)

 **Evidence:** First identified the STIG:

<https://stigaview.com/products/win11/v2r1/WN11-CC-000310/>

Initial scan result:



3. Manual Remediation Steps

Run "gpedit.msc".

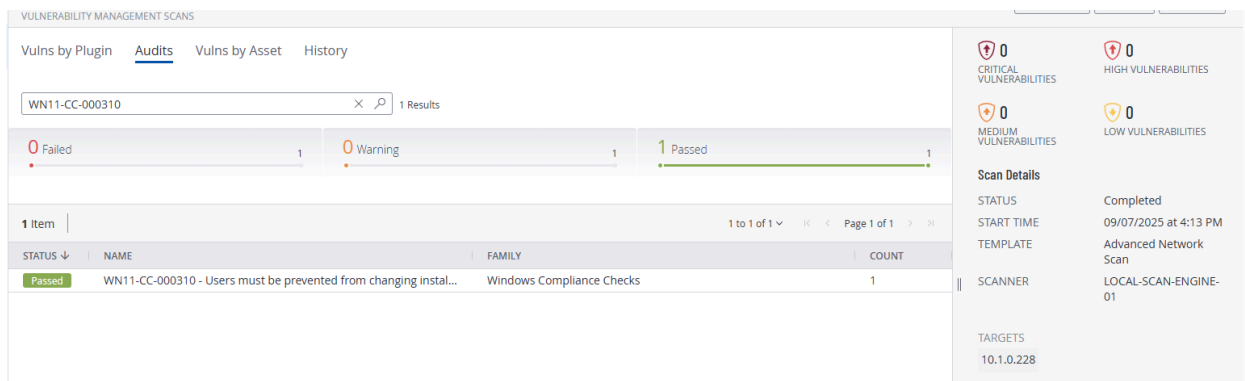
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> "Allow user control over installs" to "Disabled".

Run "gpupdate /force" and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000310
- 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: "Not Configured."
- Ran `gpupdate /force` and rescanned.

Status: Failed, Non-Compliant

Evidence:

The screenshot displays the 'VULNERABILITY MANAGEMENT SCANS' interface. The 'Audits' tab is selected, showing a search for 'WN11-CC-000310' with 1 result. A progress bar indicates 1 Failed, 0 Warning, and 0 Passed. Below this, a table lists the audit item:

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000310 - Users must be prevented from changing instal...	Windows Compliance Checks	1

On the right, the 'Scan Details' panel shows the scan is 'Completed' on 09/07/2025 at 4:28 PM, using the 'Advanced Network Scan' template and 'LOCAL-SCAN-ENGINE-01' scanner. The target is '10.1.0.228'.

5. Remediation with PowerShell Script

```
# STIG ID: WN11-CC-000310
# Prevent users from changing installation options

$regPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Installer"
$regName = "EnableUserControl"
$regValue = 0

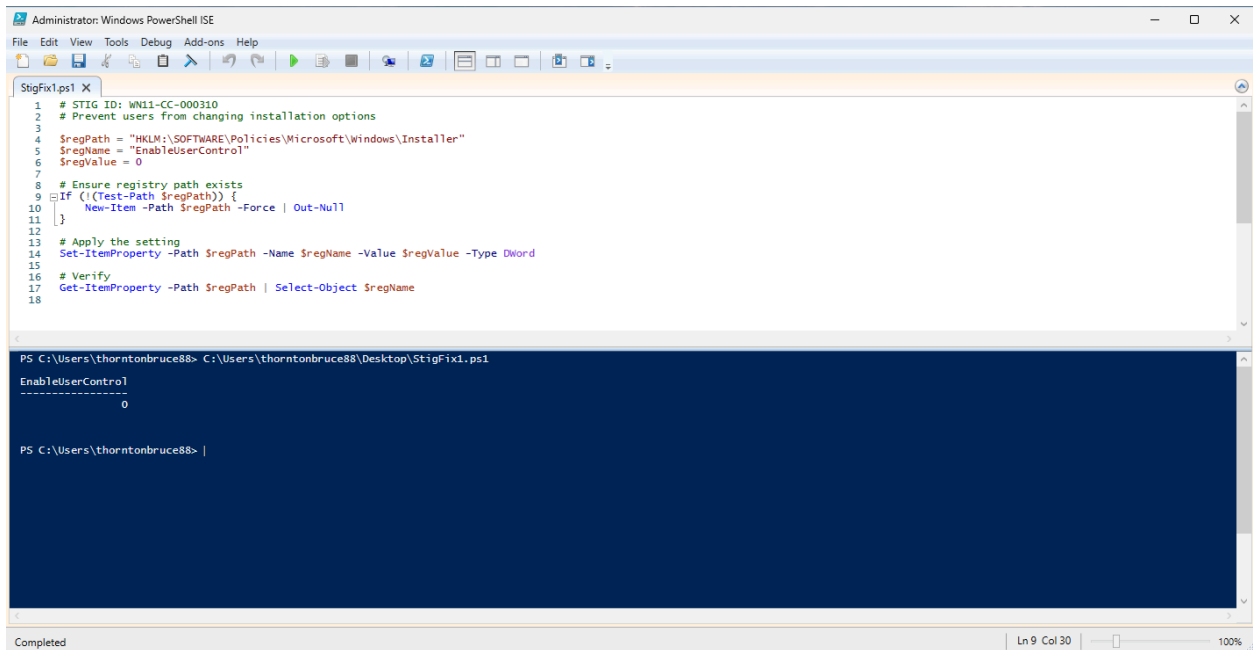
# Ensure registry path exists
If (!(Test-Path $regPath)) {
    New-Item -Path $regPath -Force | Out-Null
}
```

Apply the setting

```
Set-ItemProperty -Path $regPath -Name $regName -Value $regValue -Type DWord
```

Verify

```
Get-ItemProperty -Path $regPath | Select-Object $regName
```



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
StigFix1.ps1 X
1 # STIG ID: WN11-CC-000310
2 # Prevent users from changing installation options
3
4 $regPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Installer"
5 $regName = "EnableUserControl"
6 $regValue = 0
7
8 # Ensure registry path exists
9 If (!(Test-Path $regPath)) {
10     New-Item -Path $regPath -Force | Out-Null
11 }
12
13 # Apply the setting
14 Set-ItemProperty -Path $regPath -Name $regName -Value $regValue -Type DWord
15
16 # Verify
17 Get-ItemProperty -Path $regPath | Select-Object $regName
18

PS C:\Users\thorntonbruce88> C:\Users\thorntonbruce88\Desktop\StigFix1.ps1
EnableUserControl
-----
0

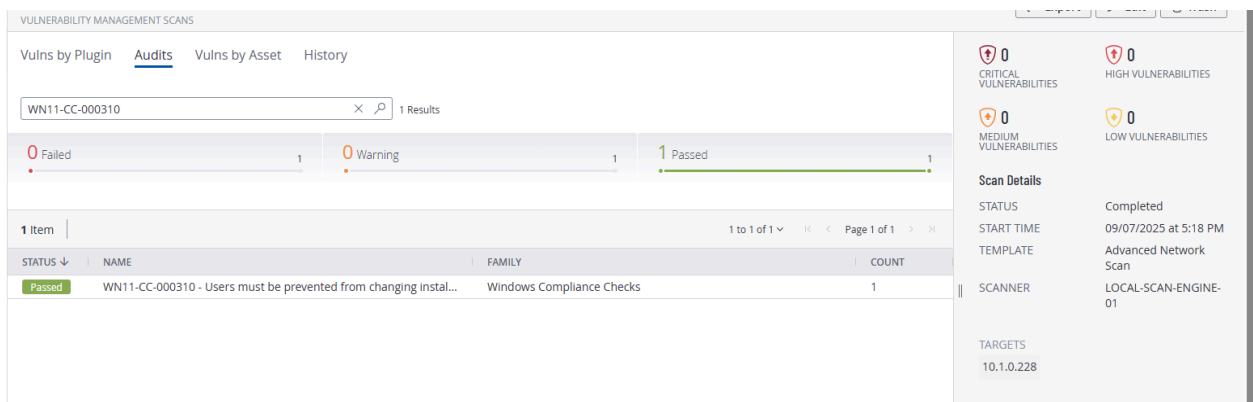
PS C:\Users\thorntonbruce88> |

Completed Ln 9 Col 30 100%
```

Ran gpupdate /force and then restart.

Status: Passed

Evidence:



VULNERABILITY MANAGEMENT SCANS

Vulns by Plugin Audits Vulns by Asset History

WN11-CC-000310 1 Results

0 Failed 1 Warning 1 Passed

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000310 - Users must be prevented from changing instal...	Windows Compliance Checks	1

1 Item 1 to 1 of 1 Page 1 of 1

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

Scan Details

STATUS Completed

START TIME 09/07/2025 at 5:18 PM

TEMPLATE Advanced Network Scan

SCANNER LOCAL-SCAN-ENGINE-01

TARGETS 10.1.0.228

6. Conclusion

The finding **WN11-CC-000310** 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 through PowerShell automation, and validated with a third scan.

This demonstrates the ability to manage Windows STIG compliance both manually and through PowerShell automation.