

STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
Date: 09/03/2025
STIG Finding: STIG ID: WN11-CC-000315
 - **SRG:** [SRG-OS-000362-GPOS-00149](#)
Severity: High
Vulnerability ID: V-253411 **CCI:** CCI-001812
-

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-000315
The Windows Installer feature "Always install with elevated privileges" must be disabled.

2. Initial Scan Results

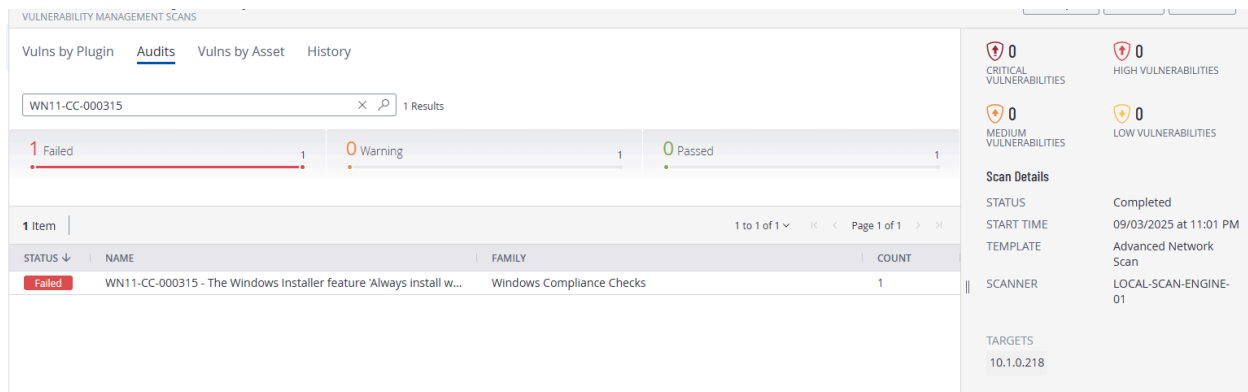
- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000315
- Status: **Fail** (non-compliant)



Evidence: First identified the STIG:

<https://stigaview.com/products/win11/v1r6/WN11-CC-000315/>

Along with initial scan results:



3. Manual Remediation Steps

Run "gpedit.msc".

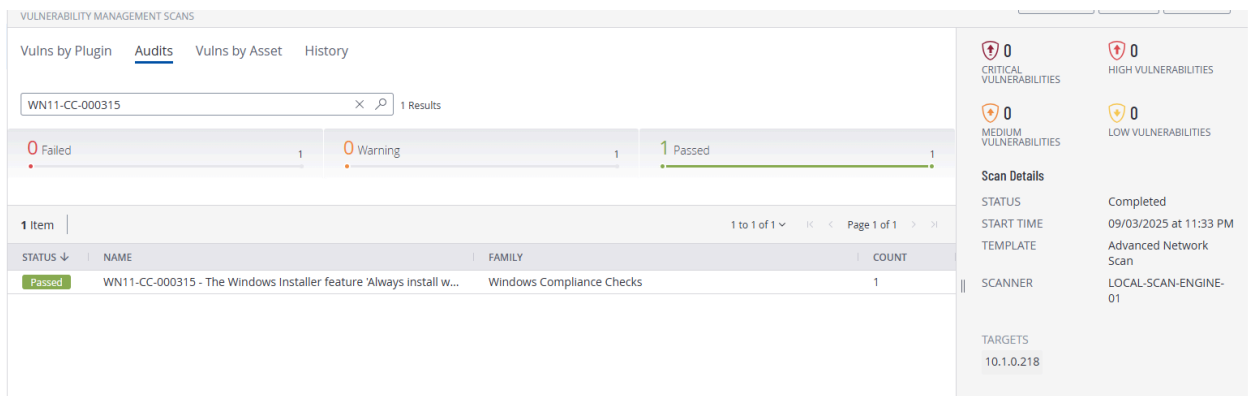
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Installer >> "Always install with elevated privileges" to "Disabled".

Run "gpupdate /force" and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000315
- 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-000315' with 1 result. A summary bar indicates 1 Failed, 0 Warning, and 0 Passed. Below this, a table lists the audit item:

| STATUS | NAME | FAMILY | COUNT |
|--------|---|---------------------------|-------|
| Failed | WN11-CC-000315 - The Windows Installer feature 'Always install w... | Windows Compliance Checks | 1 |

On the right, 'Scan Details' are shown: STATUS is 'Completed', START TIME is '09/04/2025 at 12:00 AM', TEMPLATE is 'Advanced Network Scan', SCANNER is 'LOCAL-SCAN-ENGINE-01', and TARGETS include '10.1.0.218'. A vulnerability summary on the far right shows 0 Critical, 0 High, 0 Medium, and 0 Low vulnerabilities.

5. Remediation with PowerShell Script

Ran the PowerShell script utilizing Windows PowerShell ISE:

```
# Define registry path and setting
$RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Installer"
$ValueName = "AlwaysInstallElevated"
$ValueData = 0 # Must be zero to disable privilege elevation

# Create registry key if missing
if (-not (Test-Path $RegPath)) {
    New-Item -Path $RegPath -Force | Out-Null
}

# Apply the STIG setting
```

```
Set-ItemProperty -Path $RegPath -Name $ValueName -Value $ValueData -Type DWord -Force
```

```
# Update policy (if you applied via policy path earlier)
gpupdate /force
```

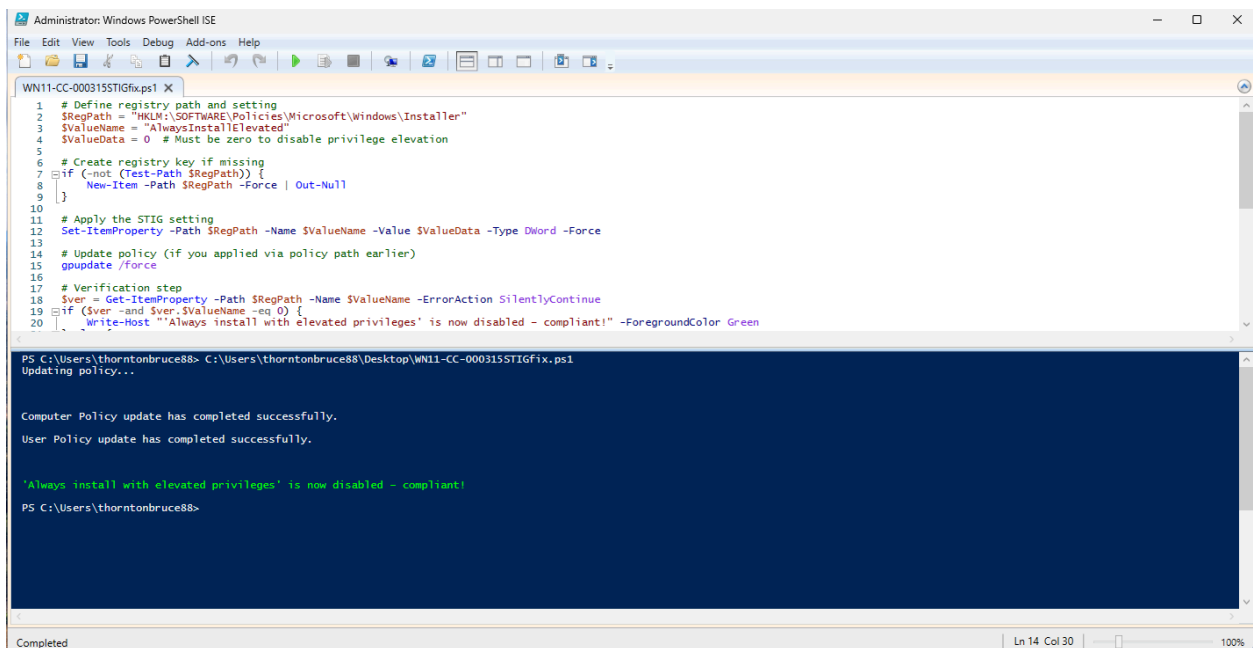
```
# Verification step
```

```
$ver = Get-ItemProperty -Path $RegPath -Name $ValueName -ErrorAction SilentlyContinue
if ($ver -and $ver.$ValueName -eq 0) {
```

```
    Write-Host "'Always install with elevated privileges' is now disabled – compliant!"
    -ForegroundColor Green
```

```
} else {
```

```
    Write-Host "Compliance not achieved. Current value:" $($ver.$ValueName) -ForegroundColor
    Red
}
```



The screenshot shows a Windows PowerShell ISE window titled "Administrator: Windows PowerShell ISE". The script being executed is "WN11-CC-000315STIGfix.ps1". The script defines a registry path and setting, creates the registry key if missing, applies the STIG setting, updates the policy, and performs a verification step. The output shows that the policy update completed successfully and the verification step confirmed that the setting is now disabled, resulting in a green message: "'Always install with elevated privileges' is now disabled – compliant!".

```
1 # Define registry path and setting
2 $RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\Installer"
3 $ValueName = "AlwaysInstallElevated"
4 $ValueData = 0 # Must be zero to disable privilege elevation
5
6 # Create registry key if missing
7 if (-not (Test-Path $RegPath)) {
8     New-Item -Path $RegPath -Force | Out-Null
9 }
10
11 # Apply the STIG setting
12 Set-ItemProperty -Path $RegPath -Name $ValueName -Value $ValueData -Type DWord -Force
13
14 # Update policy (if you applied via policy path earlier)
15 gpupdate /force
16
17 # Verification step
18 $ver = Get-ItemProperty -Path $RegPath -Name $ValueName -ErrorAction SilentlyContinue
19 if ($ver -and $ver.$ValueName -eq 0) {
20     Write-Host "'Always install with elevated privileges' is now disabled – compliant!" -ForegroundColor Green
```

PS C:\Users\thorntonbruce88> C:\Users\thorntonbruce88\Desktop\WN11-CC-000315STIGfix.ps1
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

'Always install with elevated privileges' is now disabled – compliant!
PS C:\Users\thorntonbruce88>

Evidence:

| VULNERABILITY MANAGEMENT SCANS | | | |
|---|---|---------------------------|-------|
| Vulns by Plugin Audits Vulns by Asset History | | | |
| WN11-CC-000315 1 Results | | | |
| 0 Failed | 1 | 0 Warning | 1 |
| 1 Passed | | | |
| 1 Item | | | |
| 1 to 1 of 1 Page 1 of 1 | | | |
| STATUS | NAME | FAMILY | COUNT |
| Passed | WN11-CC-000315 - The Windows Installer feature 'Always install w... | Windows Compliance Checks | 1 |

0 CRITICAL VULNERABILITIES

0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES

0 LOW VULNERABILITIES

Scan Details

STATUS: Completed

START TIME: 09/04/2025 at 8:57 AM

TEMPLATE: Advanced Network Scan

SCANNER: LOCAL-SCAN-ENGINE-01

TARGETS: 10.1.0.218

And then restart.

6. Conclusion

The finding **WN11-CC-000315** 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.