

STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
Date: 11/13/2025
STIG Finding: WN11-CC-000005
 - **SRG:** [SRG-OS-000095-GPOS-00049](#)
Severity: medium
Vulnerability ID: V-253350 **CCI:** CCI-000381
-

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-000005 "Camera access from the lock screen must be disabled."

2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000005
- Status: **Failed** (non-compliant)

 **Evidence:** First identified the STIG:

<https://stigaview.com/products/win11/v2r3/WN11-CC-000005/>

Initial scan result:

The screenshot displays the Tenable Vulnerability Management interface. At the top, the navigation bar includes 'tenable Vulnerability Management', 'Scans > Scan Details > Audit Details', and a 'Quick Actions' dropdown. The main header shows the finding ID 'WN11-CC-000005' and the title 'Camera access from the lock screen must be disabled.' with an 'AUDIT FAILED' status. Below this, there are tabs for 'Overview' and 'Assets'. A search bar and '1 Results' indicator are present. A table lists the results with columns for 'STATUS', 'NAME', and 'ACTIONS'. The table contains one entry with a 'FAILED' status and the name '10.1.0.152'. To the right of the table, there is a 'Solution' section with instructions on how to configure the policy value, a 'See Also' section with a link to a download, and a 'Reference Information' section listing various identifiers like 800-171, 3.4.6, 3.4.7, 800-53, CM-7a, CAT, II, CN-L3, 7.1.3.5(c), 8.1.4.4(a), CSF2.0, PR,PS-01, 800-171R3, 03.04.06a, 800-53R5, CM-7a, CCI, CCI-000381, CSF, and PR,IP-1, PR,PT-3, DISA_BENCHMARK, and Microsoft_Windows_11_ST.

STATUS	NAME	ACTIONS
FAILED	10.1.0.152	

3. Manual Remediation Steps

Ran gpedit.msc:

If the device does not have a camera, this is NA.

Configure the policy value for Computer Configuration >> Administrative Templates >> Control Panel >> Personalization >> "Prevent enabling lock screen camera" to "Enabled".

Run "gpupdate /force" and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000005
- Status: **Passed**

Evidence:

The screenshot displays the Tenable Vulnerability Management interface. At the top, the header shows 'tenable Vulnerability Management' and 'Scans > Scan Details'. The main content area is titled 'Win11Bruce1113DS' and 'VULNERABILITY MANAGEMENT SCANS'. It includes tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. A search bar contains 'WN11-CC-000005' with '1 Results'. Below this, a summary bar shows '0 Failed', '0 Warning', and '1 Passed'. A table lists the scan results:

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000005 - Camera access from the lock screen must be...	Windows Compliance Checks	1

On the right, a 'Scan Details' panel shows: STATUS: Completed, START TIME: 11/13/2025 at 12:13 PM, TEMPLATE: Advanced Network Scan, SCANNER: LOCAL-SCAN-ENGINE-01, and TARGETS: 10.1.0.152. Summary statistics on the right show 0 Critical, 0 High, 0 Medium, and 0 Low vulnerabilities.

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.
- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000005

Status: **Failed**, Non-Compliant

Evidence:

The screenshot shows the Tenable Vulnerability Management interface. The main header displays 'Win11Bruce1113DS' and 'VULNERABILITY MANAGEMENT SCANS'. Below this, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. The 'Audits' tab is selected, showing a search bar with 'WN11-CC-000005' and '1 Results'. A summary bar indicates 1 Failed, 0 Warning, and 0 Passed results. Below this, a table lists the audit details:

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000005 - Camera access from the lock screen must be...	Windows Compliance Checks	1

On the right side, there are summary statistics for vulnerabilities: 0 Critical, 0 High, 0 Medium, and 0 Low. Below these, the 'Scan Details' section shows the scan status as 'Completed', the start time as '11/13/2025 at 12:26 PM', the template as 'Advanced Network Scan', the scanner as 'LOCAL-SCAN-ENGINE-01', and the target as '10.1.0.152'.

5. Remediation with PowerShell Script

Save as: Remediate-WN11-CC-000005.ps1 and run **as Administrator** utilizing PowerShell ISE:

The screenshot shows a Windows PowerShell ISE window titled 'Administrator: Windows PowerShell ISE'. The script being executed is 'Remediate-WN11-CC-000005.ps1'. The script content is as follows:

```
1  
2  
3  
4 STIG ID : WN11-CC-000005  
5 Title : Camera access from the lock screen must be disabled.  
6 Check/Fix mapping:  
7 HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization  
8 NoLockScreenCamera (REG_DWORD) = 1  
9  
10  
11 $regPath = 'HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization'  
12 $valueName = 'NoLockScreenCamera'  
13 $desiredValue = 1  
14 $stigid = 'WN11-CC-000005'
```

The output of the script is displayed in the console window:

```
PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Desktop\Remediate-WN11-CC-000005.ps1  
  
ComputerName : Win11MBruce  
STIG_ID : WN11-CC-000005  
SettingName : Prevent enabling lock screen camera  
RegistryPath : HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization  
ValueName : NoLockScreenCamera  
RequiredValue : 1  
ActualValue : 1  
ComplianceStatus : Compliant  
ActionTaken : Created NoLockScreenCamera and set to 1.  
Timestamp : 11/13/2025 6:39:53 PM  
  
Completed
```

Script Used:

<#

STIG ID : WN11-CC-000005

Title : Camera access from the lock screen must be disabled.

Check/Fix mapping:

HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization

NoLockScreenCamera (REG_DWORD) = 1

#>

\$regPath = 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\Personalization'

\$valueName = 'NoLockScreenCamera'

\$desiredValue = 1

\$stigId = 'WN11-CC-000005'

Ensure key exists

if (-not (Test-Path \$regPath)) { New-Item -Path \$regPath -Force | Out-Null }

Set value if needed

\$current = Get-ItemProperty -Path \$regPath -Name \$valueName -ErrorAction SilentlyContinue

if (\$null -eq \$current) {

New-ItemProperty -Path \$regPath -Name \$valueName -PropertyType DWord -Value
\$desiredValue -Force | Out-Null

\$action = "Created \$valueName and set to \$desiredValue."

} elseif (\$current.\$valueName -ne \$desiredValue) {

Set-ItemProperty -Path \$regPath -Name \$valueName -Value \$desiredValue -Type DWord

\$action = "Updated \$valueName from \$(\$current.\$valueName) to \$desiredValue."

} else {

\$action = "\$valueName already set to \$desiredValue. No change needed."

}

Verify

\$actual = (Get-ItemProperty -Path \$regPath -Name \$valueName -ErrorAction

SilentlyContinue).\$valueName

\$compliant = if (\$actual -eq \$desiredValue) {'Compliant'} else {'Non-Compliant'}

Evidence object

[pscustomobject]@{

ComputerName = \$env:COMPUTERNAME

STIG_ID = \$stigId

SettingName = 'Prevent enabling lock screen camera'

RegistryPath = 'HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization'

ValueName = \$valueName

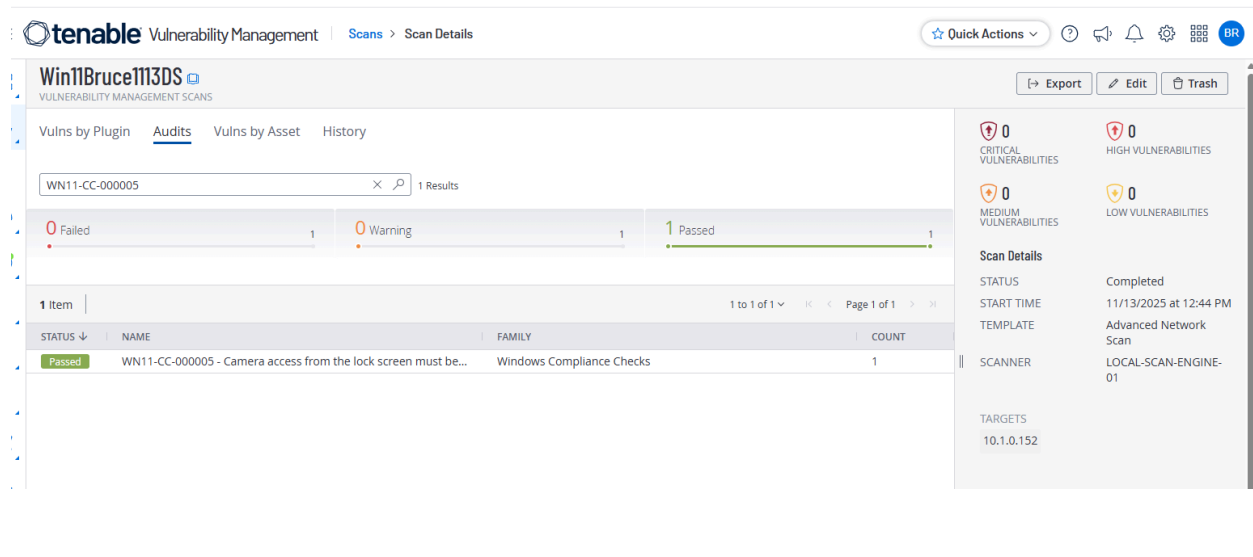
RequiredValue = \$desiredValue

ActualValue = \$actual

ComplianceStatus = \$compliant

```
ActionTaken    = $action
Timestamp      = Get-Date
} | Format-List *
```

Evidence:



6. Conclusion

The finding **WN11-CC-000005** 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.