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."

---

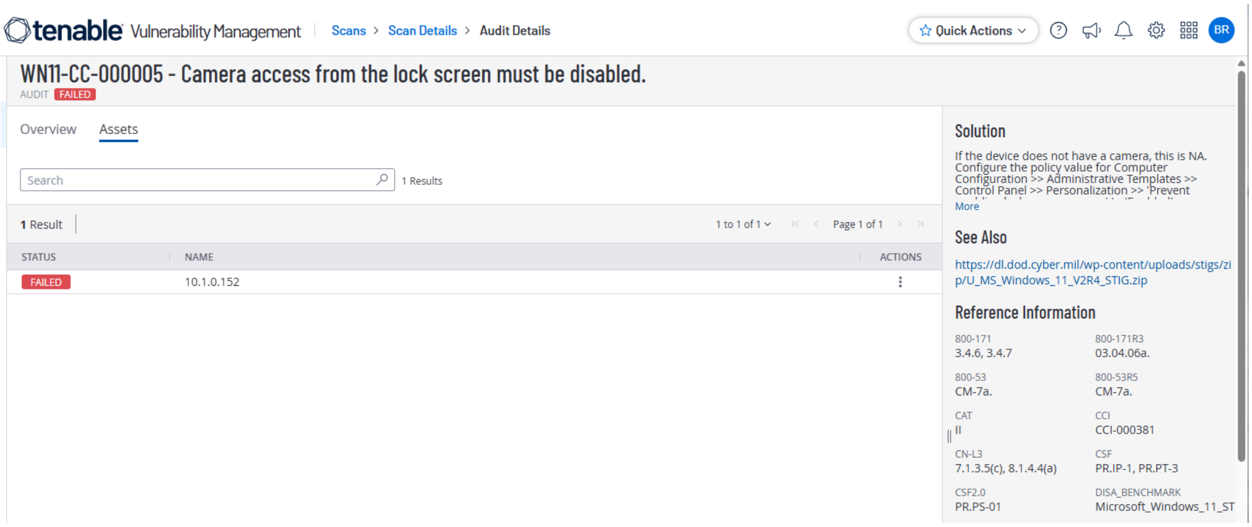
2. Initial Scan Results

- 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:



tenable Vulnerability Management
Scans > Scan Details > Audit Details
Quick Actions
BR

WN11-CC-000005 - Camera access from the lock screen must be disabled.

AUDIT FAILED

1 Results

1 Result

1 to 1 of 1

Page 1 of 1

STATUS	NAME	ACTIONS
FAILED	10.1.0.152	⋮

Solution

If the device does not have a camera, this is NA. Configure the policy value for Computer Configuration >> Administrative Templates >> Control Panel >> Personalization >> 'Prevent

More

See Also

https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

Reference Information

800-171 3.4.6, 3.4.7	800-171R3 03.04.06a.
800-53 CM-7a.	800-53R5 CM-7a.
CAT II	CCI CCI-000381
CN-L3 7.1.3.5(c), 8.1.4.4(a)	CSF PR.IP-1, PR.PT-3
CSF2.0 PR.PS-01	DISA_BENCHMARK Microsoft_Windows_11_ST

---

3. Manual Remediation Steps

Ran gpedit.msc:

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

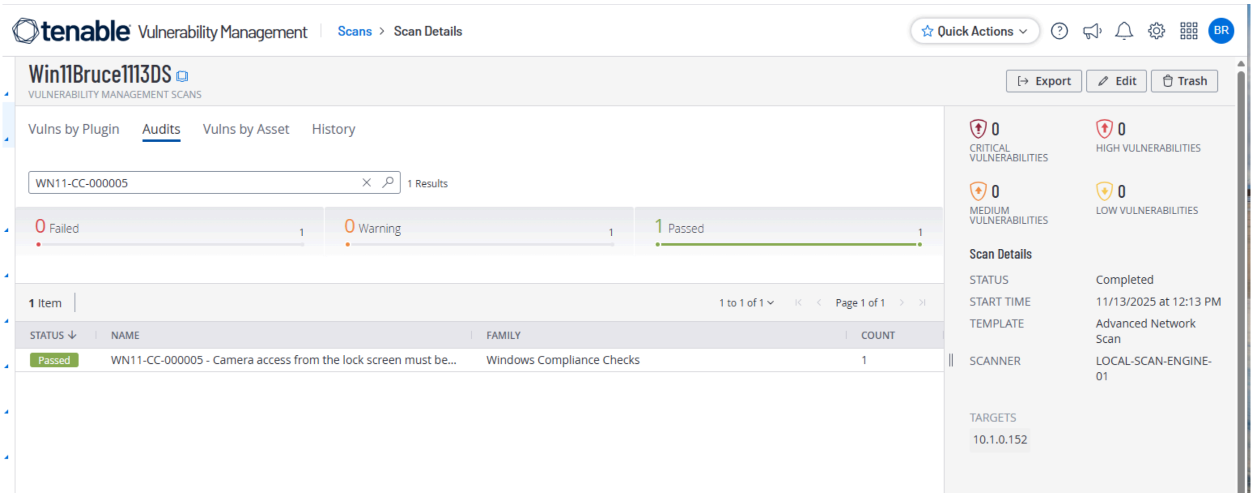
Configure the policy value for Computer Configuration >> Administrative Templates >> Control Panel >> Personalization >> "Prevent enabling lock screen camera" to "Enabled".

Run “gpupdate /force” and restart.

Scan again,

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

Evidence:



Win11Bruce1113DS
VULNERABILITY MANAGEMENT SCANS

WN11-CC-000005 — 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-000005 - Camera access from the lock screen must be...	Windows Compliance Checks	1

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

Scan Details

STATUS	Completed
START TIME	11/13/2025 at 12:13 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.152

---

4. Reintroduction of Finding (Manually Undo Test)

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

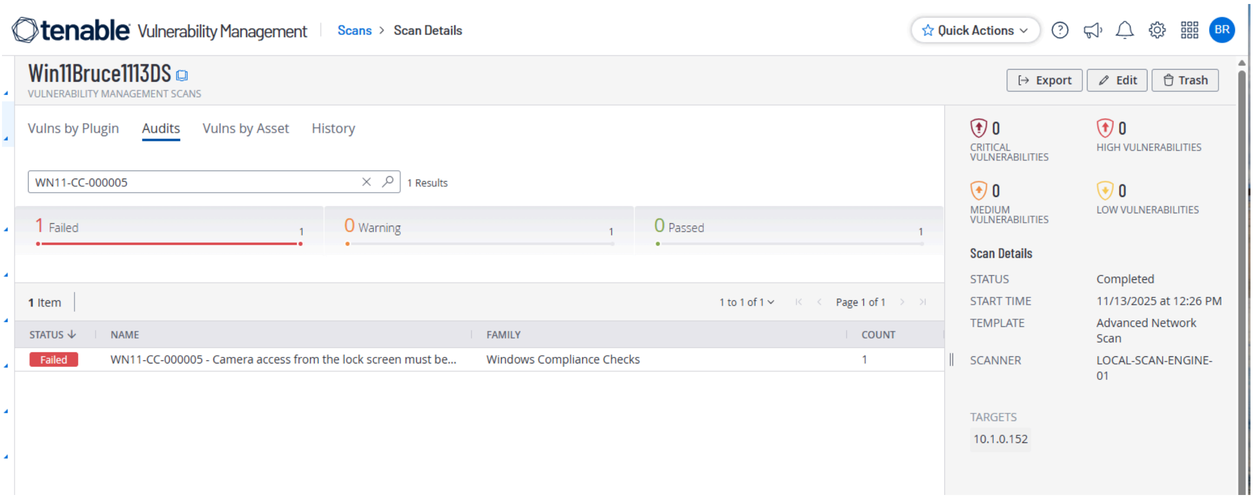
- Disabled the setting. Open Group Policy Management “gpedit.msc” and followed the instructions for remediation from before and set it to the original setting: “Not Configured”

- Ran “`gpupdate /force`” and rescanned.
- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)

- Finding ID: WN11-CC-000005

Status: **Failed**, Non-Compliant

Evidence:



Win11Bruce1113DS

VULNERABILITY MANAGEMENT SCANS

WN11-CC-000005 1 Results

1 Failed 1 | 0 Warning 1 | 0 Passed 1

1 Item | 1 to 1 of 1 | Page 1 of 1

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

0 CRITICAL VULNERABILITIES

0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES

0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	11/13/2025 at 12:26 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

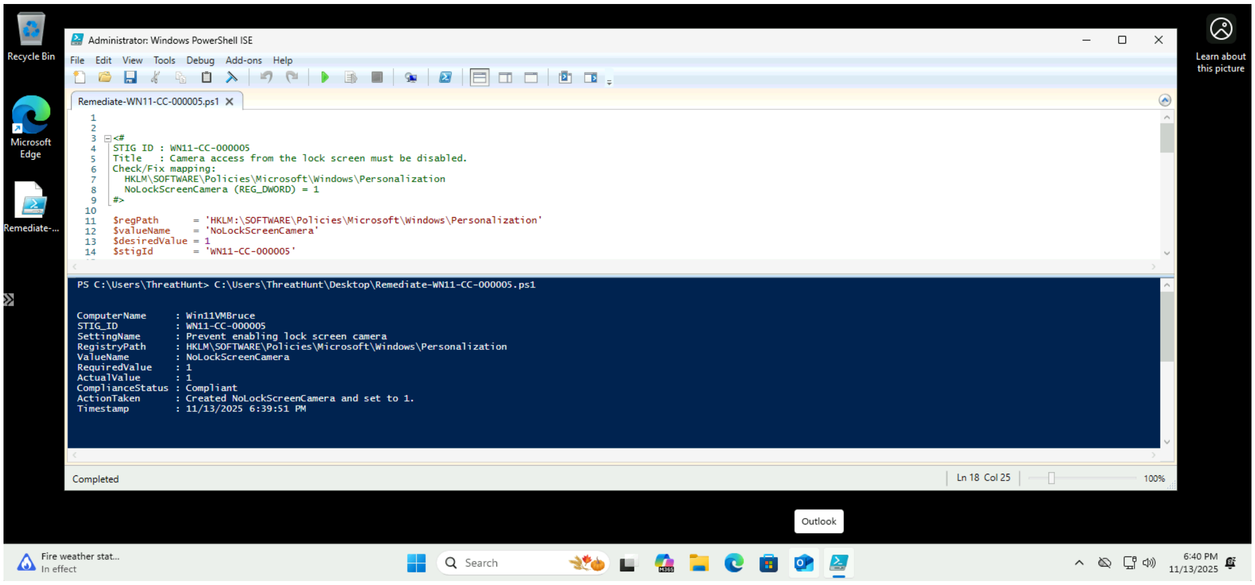
TARGETS

10.1.0.152

---

5. Remediation with PowerShell Script

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



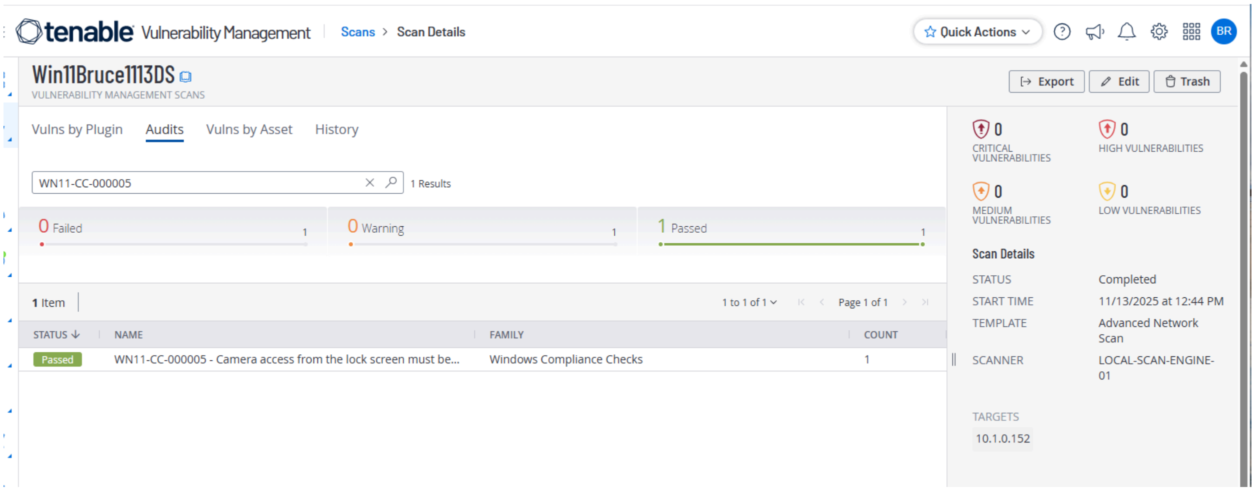
```
<#
STIG ID : WN11-CC-000005
Title   : Camera access from the lock screen must be disabled.
Check/Fix mapping:
  HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization
  NoLockScreenCamera (REG_DWORD) = 1
#>

$regPath      = 'HKLM:\SOFTWARE\Policies\Microsoft\Windows\Personalization'
$valueName    = 'NoLockScreenCamera'
$desiredValue = 1
$stigId       = 'WN11-CC-000005'
```

```
PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Desktop\Remediate-WN11-CC-000005.ps1


ComputerName     : Win11VMBruce
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 6:39:51 PM
```

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:



Win11Bruce113DS
VULNERABILITY MANAGEMENT SCANS

WN11-CC-000005 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-000005 - Camera access from the lock screen must be...	Windows Compliance Checks	1

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

Scan Details

STATUS	Completed
START TIME	11/13/2025 at 12:44 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.152

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.