STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
  Date: 10/12/2025
  STIG Finding: WN11-CC-000195
- **SRG:** SRG-OS-000480-GPOS-00227
  Severity: medium
  Vulnerability ID: V-253389 **CCI:** CCI-000366

---

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-000195 “Enhanced anti-spoofing for facial recognition must be enabled on Windows 11.”

---

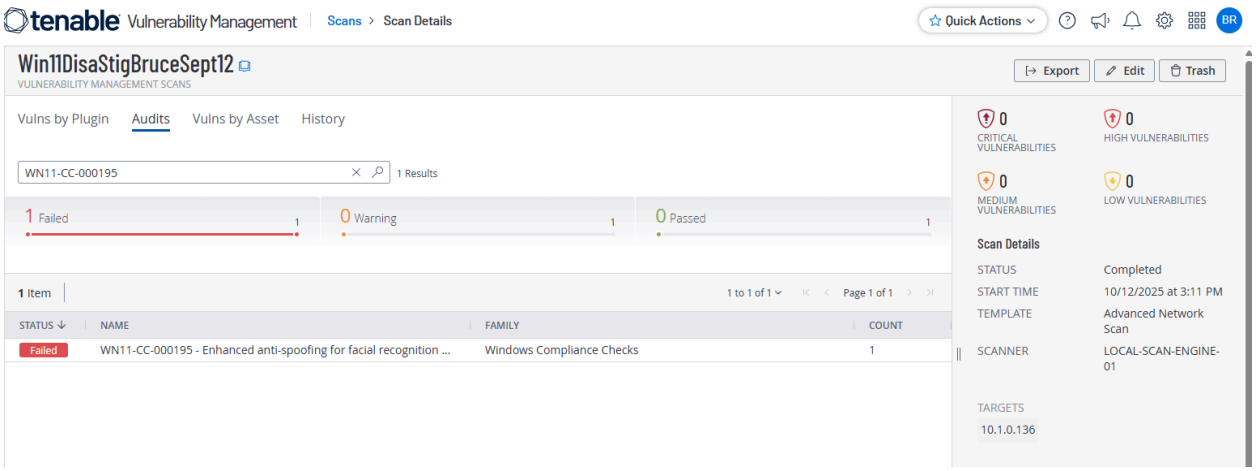
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000195
- Status: **Warning** (non-compliant)

📎 **Evidence:** First identified the STIG:

https://stigaview.com/products/win11/v2r2/WN11-CC-000195/

Initial scan result:



---

3. Manual Remediation Steps

Run “gpedit.msc”

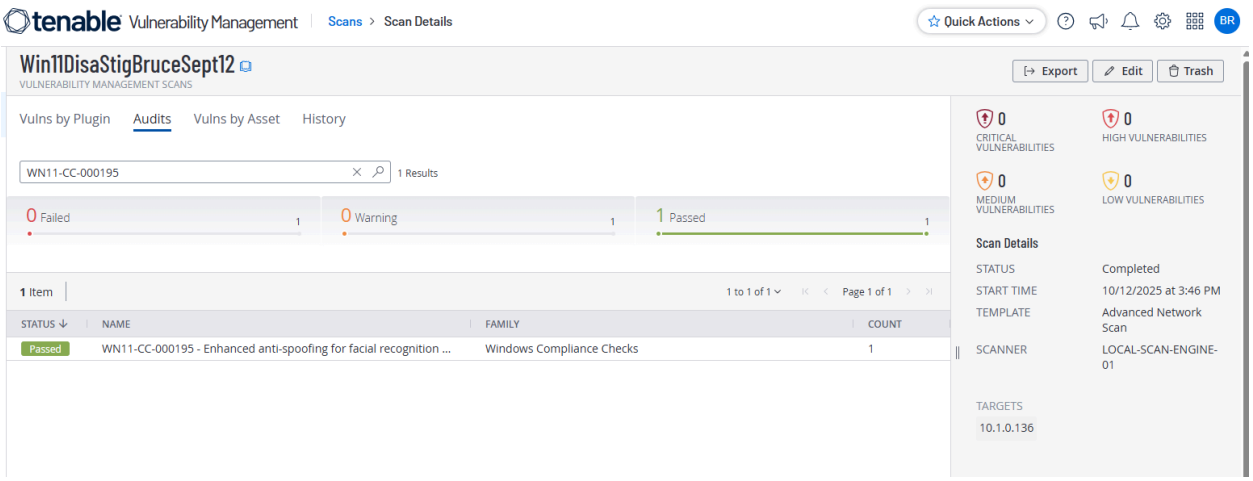
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Biometrics >> Facial Features >> "Configure enhanced anti-spoofing" to "Enabled".

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000195sudo
- Status: Passed

Evidence:



---

4. Reintroduction of Finding (Manually Undo Test)

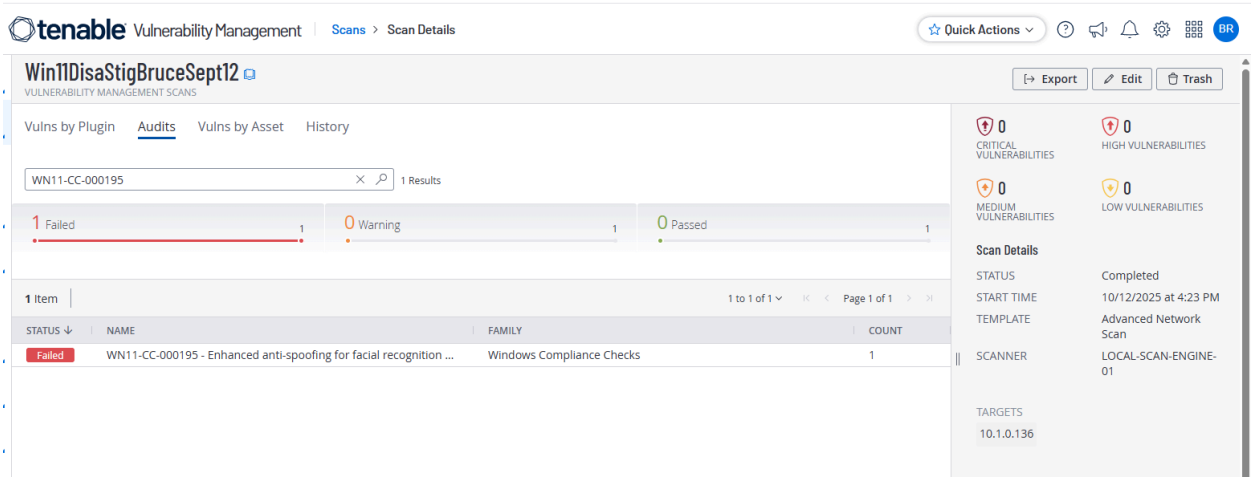
To demonstrate full control of the setting, the fix was undone:

- 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:



5. Remediation with PowerShell Script

Utilizing PowerShell ISE this script was saved and ran:

```
<#
.SYNOPSIS
  Remediates STIG WN11-CC-000195:
  Enables enhanced anti-spoofing for Windows Hello Face.

.NOTES
  Run as Administrator. A gpupdate/reboot may be required for scanners to reflect the change.
#>

# Require admin
if (-not ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()
    ).IsInRole([Security.Principal.WindowsBuiltinRole] "Administrator")) {
    Write-Error "Run this script as Administrator."
    exit 1
}

$RegPath  = "HKLM:\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatures"
$RegName  = "EnhancedAntiSpoofing"
$RegValue = 1

# Ensure path exists
if (-not (Test-Path $RegPath)) {
    New-Item -Path $RegPath -Force | Out-Null
    Write-Output "Created registry path: $RegPath"
}

# Set value
New-ItemProperty -Path $RegPath -Name $RegName -Value $RegValue -PropertyType DWord
-Force | Out-Null
Write-Output "Set $RegName to $RegValue at $RegPath"

# Optional: force policy refresh
gpupdate /target:computer /force | Out-Null

# Verify
```

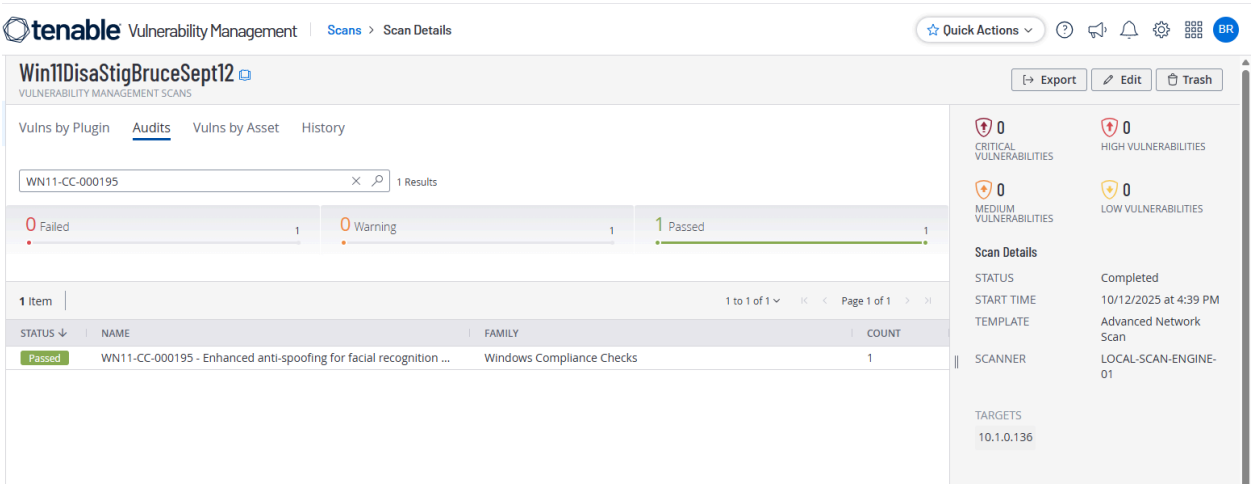
```
$current = (Get-ItemProperty -Path $RegPath -Name $RegName -ErrorAction
SilentlyContinue).$RegName
if ($current -eq $RegValue) {
    Write-Output "✅ Enhanced anti-spoofing policy is enabled."
} else {
    Write-Error "❌ Failed to enable enhanced anti-spoofing (current: $current)."
}
```

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000204
- Status: Passed

Evidence:



- **Note:** Passing compliance also depends on the device supporting Windows Hello Face with anti-spoofing (IR camera). If hardware doesn’t support it, scanners can still flag it even with the key set—in that case you’d document a waiver/POA&M.

---

6. Conclusion

The finding **WN11-CC-000195** 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.