STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
  Date: 11/3/2025
  STIG Finding: WN11-CC-000252
- **SRG:** SRG-OS-000095-GPOS-00049
  Severity: medium
  Vulnerability ID: V-253399 **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-000252 “Windows 11 must be configured to disable Windows Game Recording and Broadcasting.”

---

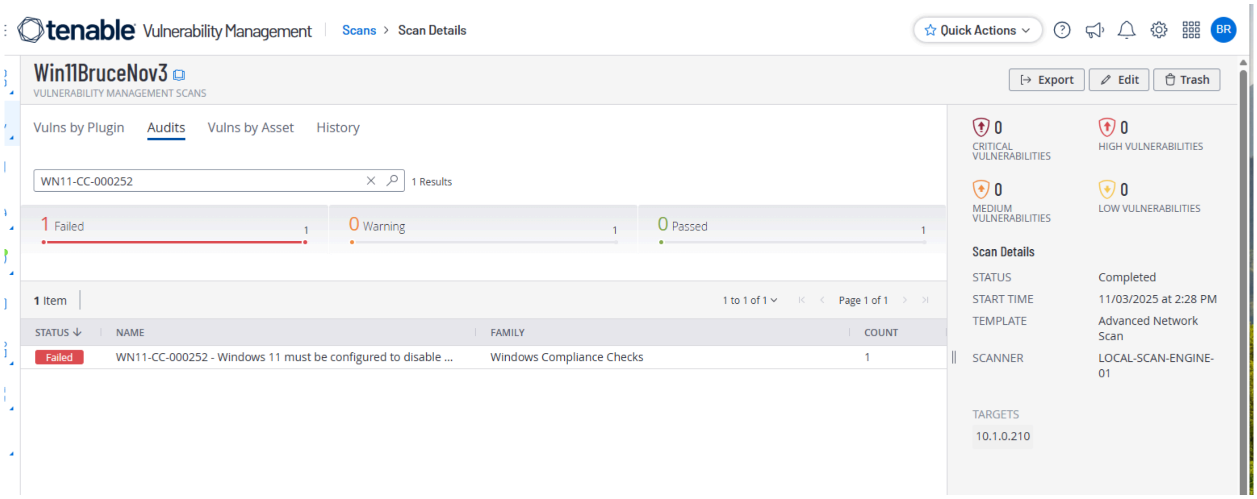
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000252
- Status: **Failed** (non-compliant)

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

https://stigaview.com/products/win11/v2r1/WN11-CC-000252/

Initial scan result:



Win11BruceNov3
VULNERABILITY MANAGEMENT SCANS

WN11-CC-000252 — 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-000252 - Windows 11 must be configured to disable ...	Windows Compliance Checks	1

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

Scan Details

STATUS	Completed
START TIME	11/03/2025 at 2:28 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.0.210

3. Manual Remediation Steps

Run “gpedit.msc”

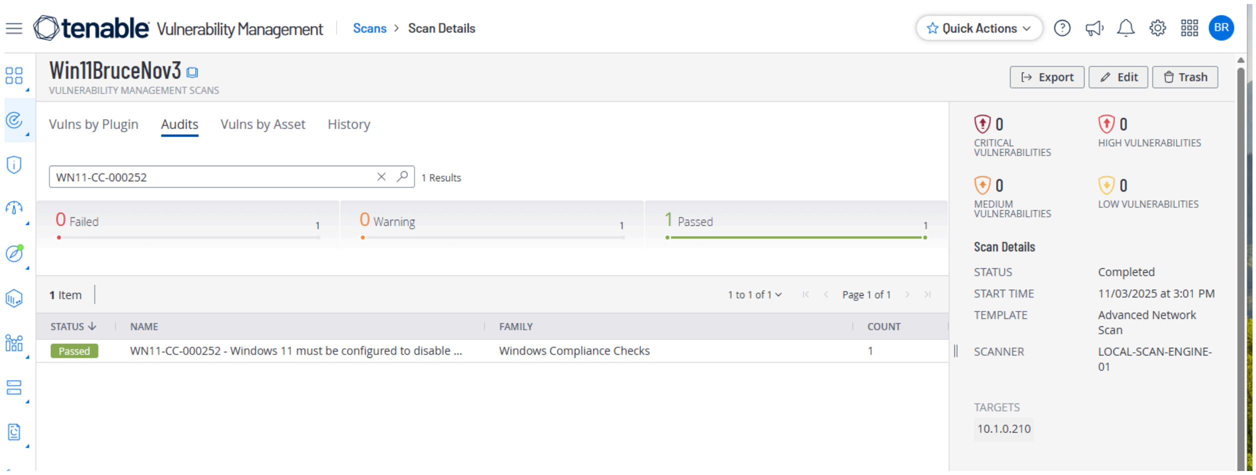
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Game Recording and Broadcasting >> "Enables or disables Windows Game Recording and Broadcasting" to "Disabled"

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000252
- Status: **Passed**

Evidence:



tenable Vulnerability Management | Scans > Scan Details

Quick Actions

Win11BruceNov3

VULNERABILITY MANAGEMENT SCANS

Export | Edit | Trash

Vulns by Plugin | Audits | Vulns by Asset | History

WN11-CC-000252 — 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-000252 - Windows 11 must be configured to disable ...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES | 0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES | 0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	11/03/2025 at 3:01 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

10.1.0.210

---

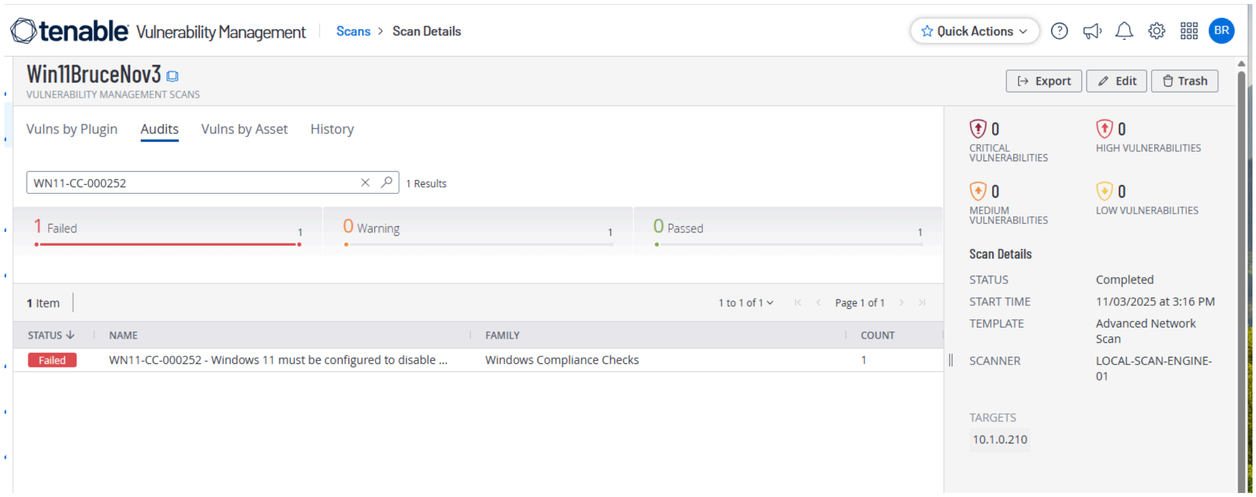
4. Reintroduction of Finding (Manually Undo Test)

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:



tenable Vulnerability Management | Scans > Scan Details

Quick Actions

Win11BruceNov3

VULNERABILITY MANAGEMENT SCANS

Export | Edit | Trash

Vulns by Plugin | Audits | Vulns by Asset | History

WN11-CC-000252 — 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-000252 - Windows 11 must be configured to disable ...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES | 0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES | 0 LOW VULNERABILITIES

Scan Details

STATUS	Completed
START TIME	11/03/2025 at 3:16 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

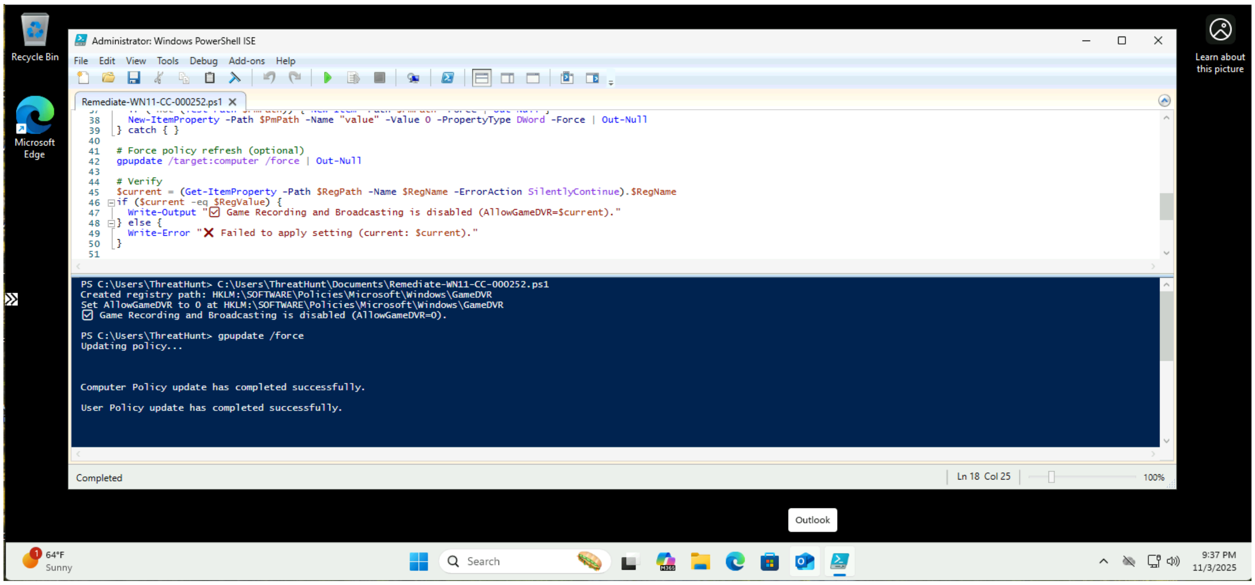
10.1.0.210

5. Remediation with PowerShell Script

Save as: `Remediate-WN11-CC-000252.ps1` and run **as Administrator** utilizing PowerShell ISE:

```
<#
.SYNOPSIS
  Remediates STIG WN11-CC-000252:
  Disables Windows Game Recording and Broadcasting (GameDVR).

.NOTES
  - Run as Administrator.
  - Tenable/Nessus typically checks
HKLM\SOFTWARE\Policies\Microsoft\Windows\GameDVR\AllowGameDVR = 0.
  - A gpupdate/reboot or logoff may be needed before the UI reflects 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
}

# Primary policy key (what compliance tools look for)
$RegPath  = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\GameDVR"
$RegName  = "AllowGameDVR"
$RegValue = 0

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

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

# (Optional) Also set MDM PolicyManager path for defense-in-depth on some builds
try {
  $PmPath = "HKLM:\SOFTWARE\Microsoft\PolicyManager\default\ApplicationManagement\AllowGameDVR"
  if (-not (Test-Path $PmPath)) { New-Item -Path $PmPath -Force | Out-Null }
  New-ItemProperty -Path $PmPath -Name "value" -Value 0 -PropertyType DWord -Force | Out-Null
} catch { }

# Force policy refresh (optional)
gpupdate /target:computer /force | Out-Null

# Verify
$current = (Get-ItemProperty -Path $RegPath -Name $RegName -ErrorAction SilentlyContinue).$RegName
if ($current -eq $RegValue) {
  Write-Output "✅ Game Recording and Broadcasting is disabled (AllowGameDVR=$current)."
} else {
  Write-Error "❌ Failed to apply setting (current: $current)."
}
```

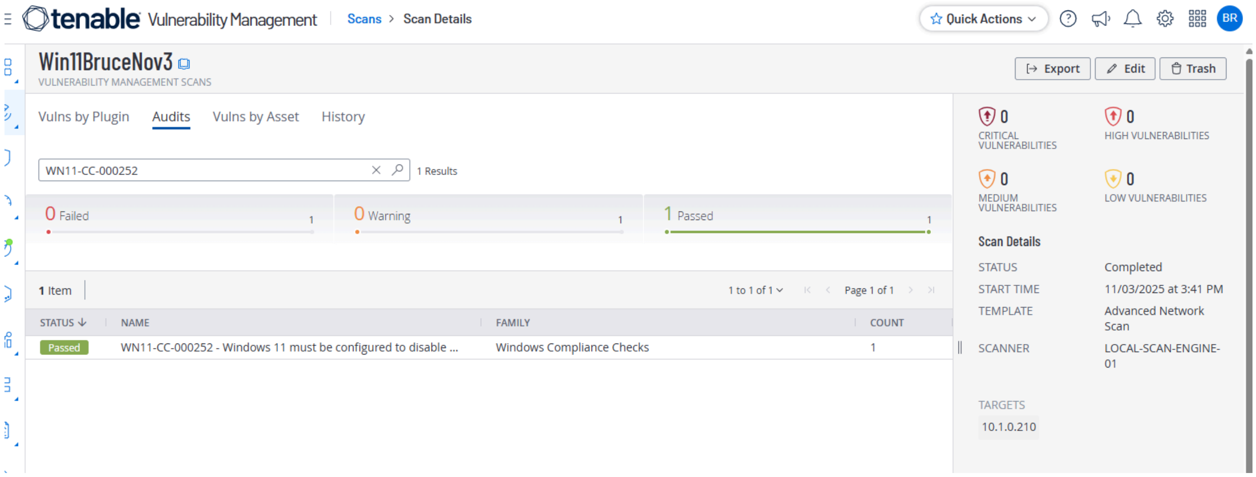
Evidence:



```
  New-ItemProperty -Path $PmPath -Name "value" -Value 0 -PropertyType DWord -Force | Out-Null
} catch { }

# Force policy refresh (optional)
gpupdate /target:computer /force | Out-Null

# Verify
$current = (Get-ItemProperty -Path $RegPath -Name $RegName -ErrorAction SilentlyContinue).$RegName
if ($current -eq $RegValue) {
  Write-Output "☑ Game Recording and Broadcasting is disabled (AllowGameDVR=$current)."
} else {
  Write-Error "✗ Failed to apply setting (current: $current)."
}
```

```
PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Documents\Remediate-WN11-CC-000252.ps1
Created registry path: HKLM:\SOFTWARE\Policies\Microsoft\Windows\GameDVR
Set AllowGameDVR to 0 at HKLM:\SOFTWARE\Policies\Microsoft\Windows\GameDVR
☑ Game Recording and Broadcasting is disabled (AllowGameDVR=0).

PS C:\Users\ThreatHunt> gpupdate /force
Updating policy...



Computer Policy update has completed successfully.

User Policy update has completed successfully.
```

Evidence:



Win11BruceNov3

VULNERABILITY MANAGEMENT SCANS

WN11-CC-000252 — 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-000252 - Windows 11 must be configured to disable ...	Windows Compliance Checks	1

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

Scan Details

STATUS	Completed
START TIME	11/03/2025 at 3:41 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

10.1.0.210

6. Conclusion

The finding **WN11-CC-000252** 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.