

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:

The screenshot shows the Tenable Vulnerability Management interface. At the top, it displays the scan name "Win11BruceNov3" and the status "VULNERABILITY MANAGEMENT SCANS". Below this, there are tabs for "Vulns by Plugin", "Audits" (which is selected), "Vulns by Asset", and "History". A search bar shows the query "WN11-CC-000252" with 1 result found. The results table has columns for STATUS (Failed, Warning, Passed), NAME, FAMILY, and COUNT. One row is shown: "Failed" for "WN11-CC-000252 - Windows 11 must be configured to disable ...", under the "Windows Compliance Checks" family, with a count of 1. To the right of the results table are summary counts for Critical, High, Medium, and Low vulnerabilities. On the far right, "Scan Details" are listed, including Status (Completed), Start Time (11/03/2025 at 2:28 PM), Template (Advanced Network Scan), Scanner (LOCAL-SCAN-ENGINE-01), and 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:

The screenshot shows the Tenable Vulnerability Management interface. The scan name is "Win11BruceNov3". The audit results show 0 Failed, 0 Warning, and 1 Passed. The passed item is "WN11-CC-000252 - Windows 11 must be configured to disable ...". The scan details indicate it was completed on 11/03/2025 at 3:01 PM using the "Advanced Network Scan" template and the "LOCAL-SCAN-ENGINE-01" scanner, targeting the IP 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:

The screenshot shows the Tenable Vulnerability Management interface. The scan name is "Win11BruceNov3". The audit results show 1 Failed, 0 Warning, and 0 Passed. The failed item is "WN11-CC-000252 - Windows 11 must be configured to disable ...". The scan details indicate it was completed on 11/03/2025 at 3:16 PM using the "Advanced Network Scan" template and the "LOCAL-SCAN-ENGINE-01" scanner, targeting the IP 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 {
```

```

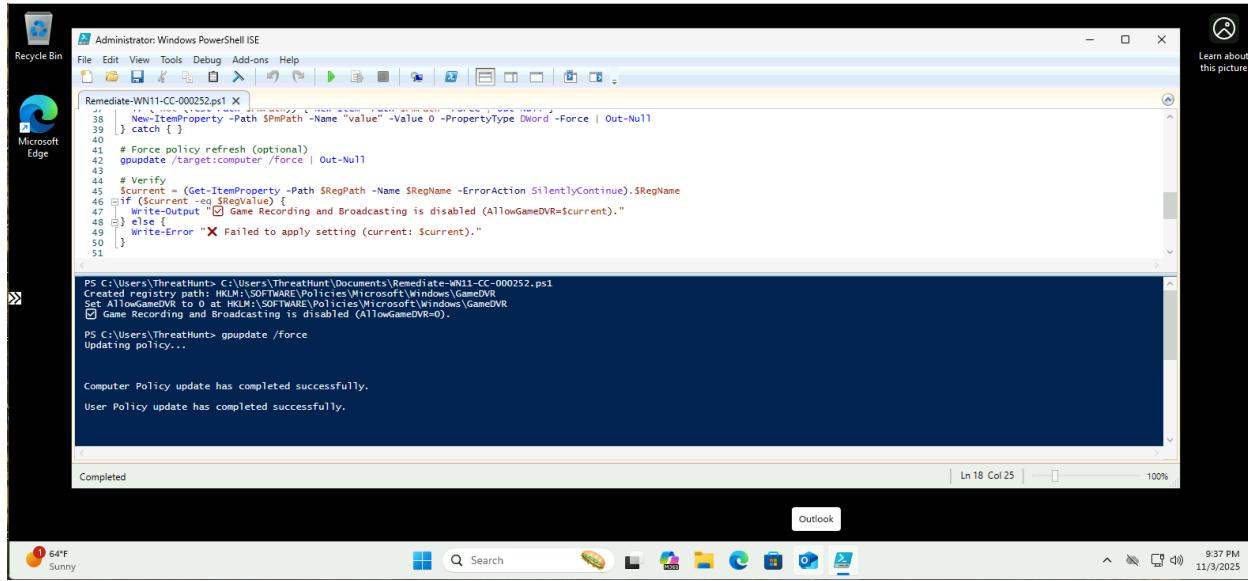
$PmPath =
"HKLM:\SOFTWARE\Microsoft\PolicyManager\default\ApplicationManagement\AllowGameDVR
"
if (-not (Test-Path $PmPath)) { New-Item -Path $PmPath -Force | Out-Null }
    New-ItemProperty -Path $PmPath -Name "value" -Value 0 -PropertyType DWord -Force |
Out-Null
} catch {}

# 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:



The screenshot shows a Windows PowerShell window titled 'Administrator: Windows PowerShell ISE'. The script 'Remediate-WN11-CC-000252.ps1' is running, with lines 38-51 visible. The output pane shows the command being run and its results:

```

PS C:\Users\ThreatHunt> .\Remediate-WN11-CC-000252.ps1
Created registry path: HKLM:\SOFTWARE\Microsoft\Windows\GameDVR
Set AllowGameDVR to 0 at HKLM:\SOFTWARE\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.

Completed

```

The status bar at the bottom right indicates the time is 9:37 PM on 11/3/2025.

Evidence:

The screenshot shows the Tenable Vulnerability Management interface. At the top, it displays 'Vulnerability Management' and 'Scans > Scan Details'. The main area is titled 'Win11BruceNov3' and shows a search result for 'WN11-CC-000252' with 1 result found. The results table has columns for STATUS, NAME, FAMILY, and COUNT. One row is shown: 'Passed' for 'WN11-CC-000252 - Windows 11 must be configured to disable ...' under 'Windows Compliance Checks' with a count of 1. On the right side, there's a summary of vulnerabilities: 0 Critical, 0 High, 0 Medium, and 0 Low. Below that is a 'Scan Details' section with information like Status: Completed, Start Time: 11/03/2025 at 3:41 PM, Template: Advanced Network Scan, Scanner: LOCAL-SCAN-ENGINE-01, and Target: 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.