

STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
Date: 11/2/2025
STIG Finding: WN11-CC-000197
 - **SRG:** [SRG-OS-000095-GPOS-00049](#)
Severity: medium
Vulnerability ID: V-253436 **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-000197 “Microsoft consumer experiences must be turned off.”

2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000197
- Status: **Failed** (non-compliant)



Evidence: First identified the STIG:

<https://stigaview.com/products/win11/v1r5/WN11-CC-000197/>

Initial scan result

Vulnerability Management | Scans > Scan Details

Win11BruceNov2

VULNERABILITY MANAGEMENT SCANS

Audits

Vulns by Asset

History

WN11-CC-000197

1 Failed | 0 Warning | 0 Passed

1 Item

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000197 - Microsoft consumer experiences must be tu...	Windows Compliance Checks	1

Scan Details

STATUS	Completed
START TIME	11/02/2025 at 8:47 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01
TARGETS	10.1.0.22

3. Manual Remediation Steps

Run “gpedit.msc”

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Cloud Content >> "Turn off Microsoft consumer experiences" to "Enabled".

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000197
- Status: **Passed**

Evidence:

The screenshot shows the Tenable Vulnerability Management interface. The scan name is "Win11BruceNov2". The audit results table shows 1 item: "WN11-CC-000197 - Microsoft consumer experiences must be tu..." under the Windows Compliance Checks family, with a status of Passed. The right sidebar displays scan details: Status Completed, Start Time 11/02/2025 at 9:31 PM, Template Advanced Network Scan, Scanner LOCAL-SCAN-ENGINE-01, and Target 10.1.0.22. The sidebar also shows vulnerability counts: 0 Critical, 0 High, 0 Medium, and 0 Low.

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 "Win11BruceNov2". The audit results table shows 1 item: "WN11-CC-000197 - Microsoft consumer experiences must be tu..." under the Windows Compliance Checks family, with a status of Failed. The right sidebar displays scan details: Status Completed, Start Time 11/02/2025 at 9:50 PM, Template Advanced Network Scan, Scanner LOCAL-SCAN-ENGINE-01, and Target 10.1.0.22. The sidebar also shows vulnerability counts: 1 Critical, 0 High, 0 Medium, and 0 Low.

5. Remediation with PowerShell Script

Save as: Remediate-WN11-CC-000197.ps1 and run **as Administrator** utilizing PowerShell ISE:

```
<#
.SYNOPSIS
Remediates STIG WN11-CC-000197:
Turns off Microsoft consumer experiences (Cloud Content).

.NOTES
Run as Administrator. A gpupdate/reboot may be needed before scanners 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\Windows\CloudContent"

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

# Set policy value (primary key used by GPO/Tenable)
New-ItemProperty -Path $RegPath -Name "DisableWindowsConsumerFeatures" -Value 1 -PropertyType DWord -Force | Out-Null

# (Optional) Set legacy alias some environments also read
New-ItemProperty -Path $RegPath -Name "DisableConsumerFeatures" -Value 1 -PropertyType DWord -Force | Out-Null

Write-Output "✅ Microsoft consumer experiences disabled."

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

```

# Verify
$primary = (Get-ItemProperty -Path $RegPath -Name "DisableWindowsConsumerFeatures"
-ErrorAction SilentlyContinue).DisableWindowsConsumerFeatures
$alias  = (Get-ItemProperty -Path $RegPath -Name "DisableConsumerFeatures" -ErrorAction
SilentlyContinue).DisableConsumerFeatures
Write-Output ("Verification: DisableWindowsConsumerFeatures={0};"
DisableConsumerFeatures={1}" -f $primary,$alias)

```

Evidence:

```

Administrator: Windows PowerShell IE
File Edit View Tools Debug Add-ons Help
Recycle Bin
Microsoft Edge
Remediate...
Remediate-WN11-CC-000197.ps1 X
27 # (Optional) Set legacy alias some environments also read
28 New-ItemProperty -Path $RegPath -Name "DisableConsumerFeatures" -Value 1 -PropertyType Dword -Force | Out-Null
29
30 Write-Output "Microsoft consumer experiences disabled."
31
32 # Force policy refresh (optional)
33 gpupdate /target:computer /force | Out-Null
34
35 # Verify
36 $primary = (Get-ItemProperty -Path $RegPath -Name "DisableWindowsConsumerFeatures" -ErrorAction SilentlyContinue).DisableWindowsConsumerFeatures
37 $alias  = (Get-ItemProperty -Path $RegPath -Name "DisableConsumerFeatures" -ErrorAction SilentlyContinue).DisableConsumerFeatures
38 Write-Output ("Verification: DisableWindowsConsumerFeatures={0}; DisableConsumerFeatures={1}" -f $primary,$alias)
40

PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Desktop\Remediate-WN11-CC-000197.ps1
[Truncated]
PS C:\Users\ThreatHunt> gpupdate /force
Updating policy...
Computer Policy update has completed successfully.
User Policy update has completed successfully.

Completed
Ln 18 Col 25 100%
Outlook
1 inch of rain
Tonight
4:03 AM
11/3/2025

```

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000197
- Status: **Passed**

Evidence:

The screenshot shows the Tenable Vulnerability Management interface. The top navigation bar includes 'Scans' and 'Scan Details'. The main content area is titled 'Win11BruceNov2 VULNERABILITY MANAGEMENT SCANS'. A search bar displays 'WN11-CC-000197' with '1 Results'. Below the search is a summary bar with counts: 0 Failed, 0 Warning, and 1 Passed. A detailed table follows, showing 1 item with status 'Passed', name 'WN11-CC-000197 - Microsoft consumer experiences must be tu...', family 'Windows Compliance Checks', and count 1. To the right, a 'Scan Details' sidebar provides completed information: Start Time (11/02/2025 at 10:08 PM), Template (Advanced Network Scan), Scanner (LOCAL-SCAN-ENGINE-01), and Target (10.1.0.22). The sidebar also displays vulnerability counts: 0 Critical, 0 High, 0 Medium, and 0 Low.

6. Conclusion

The finding **WN11-CC-000197** 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.