

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."

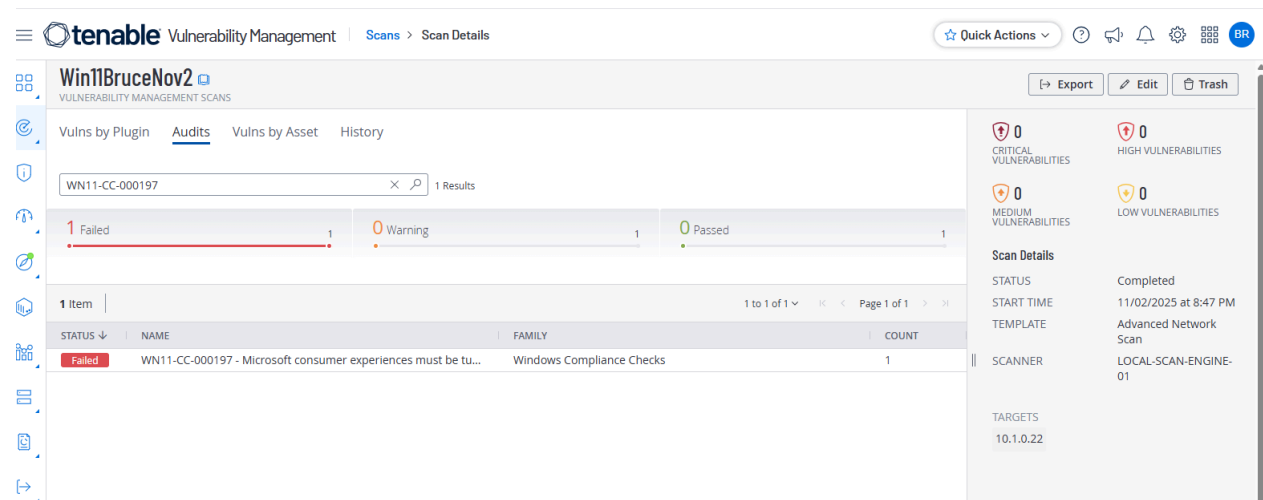
2. Initial Scan Results

- 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



tenable Vulnerability Management | Scans > Scan Details

Win11BruceNov2
VULNERABILITY MANAGEMENT SCANS

Vulns by Plugin | Audits | Vulns by Asset | History

WN11-CC-000197 1 Results

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 top navigation bar includes 'tenable Vulnerability Management' and 'Scans > Scan Details'. The main header displays 'Win11BruceNov2' and 'VULNERABILITY MANAGEMENT SCANS'. The left sidebar contains navigation icons. The main content area shows the 'Audits' tab selected, with a search bar containing 'WN11-CC-000197' and '1 Results'. Below the search bar, there are three progress bars: 'Failed' (0), 'Warning' (0), and 'Passed' (1). A table lists the scan results:

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

On the right side, the 'Scan Details' panel shows the following information:

- CRITICAL VULNERABILITIES: 0
- HIGH VULNERABILITIES: 0
- MEDIUM VULNERABILITIES: 0
- LOW VULNERABILITIES: 0
- STATUS: Completed
- START TIME: 11/02/2025 at 9:31 PM
- TEMPLATE: Advanced Network Scan
- SCANNER: LOCAL-SCAN-ENGINE-01
- TARGETS: 10.1.0.22

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 top navigation bar includes 'tenable Vulnerability Management' and 'Scans > Scan Details'. The main header displays 'Win11BruceNov2' and 'VULNERABILITY MANAGEMENT SCANS'. The left sidebar contains navigation icons. The main content area shows the 'Audits' tab selected, with a search bar containing 'WN11-CC-000197' and '1 Results'. Below the search bar, there are three progress bars: 'Failed' (1), 'Warning' (0), and 'Passed' (0). A table lists the scan results:

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

On the right side, the 'Scan Details' panel shows the following information:

- CRITICAL VULNERABILITIES: 0
- HIGH VULNERABILITIES: 0
- MEDIUM VULNERABILITIES: 0
- LOW VULNERABILITIES: 0
- STATUS: Completed
- START TIME: 11/02/2025 at 9:50 PM
- TEMPLATE: Advanced Network Scan
- SCANNER: LOCAL-SCAN-ENGINE-01
- TARGETS: 10.1.0.22

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
```

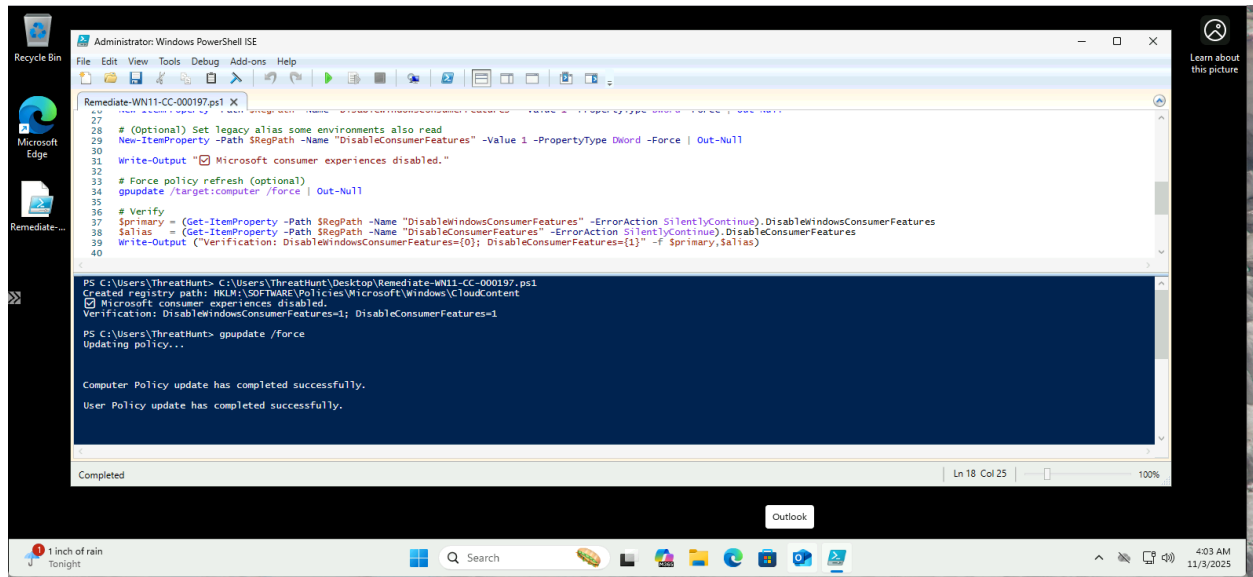
Verify

```
$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:



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 displays the Tenable Vulnerability Management interface. The top navigation bar includes the Tenable logo, 'Vulnerability Management', and a breadcrumb trail 'Scans > Scan Details'. A 'Quick Actions' dropdown menu is visible on the right. The main header shows the scan name 'Win11BruceNov2' and 'VULNERABILITY MANAGEMENT SCANS'. Below this, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. A search bar contains 'WN11-CC-000197' with '1 Results' indicated. A summary bar shows '0 Failed', '0 Warning', and '1 Passed'. The main table lists one item with the following details:

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

On the right side, a 'Scan Details' panel provides additional information:

- Vulnerability Counts:** 0 Critical, 0 High, 0 Medium, 0 Low vulnerabilities.
- Status:** Completed
- Start Time:** 11/02/2025 at 10:08 PM
- Template:** Advanced Network Scan
- Scanner:** LOCAL-SCAN-ENGINE-01
- Targets:** 10.1.0.22

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.