

STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
Date: 12/1/2025
STIG Finding: WN11-CC-000105
 - **SRG:** SRG-OS-000095-GPOS-00049
Severity: medium
Vulnerability ID: V-253375 **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-000105 “Web publishing and online ordering wizards must be prevented from downloading a list of providers.”

2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000105
- Status: **Failed** (non-compliant)



Evidence: First identified the STIG:

<https://stigaview.com/products/win11/v1r6/WN11-CC-000105/>

Initial scan result:

The screenshot shows the Tenable Vulnerability Management interface. At the top, it says "Scans > Scan Details > Audit Details". Below that, the title "WN11-CC-000105 - Web publishing and online ordering wizards must be prevented from downloading a list of pr..." is displayed. A red "AUDIT FAILED" badge is visible. The main area shows a table with one result, where the status is "FAILED" and the name is "10.1.0.169". On the right side, there's a "Solution" section with a detailed configuration path: "Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Internet Communication Management >> Internet Communication settings >> 'Turn off Internet download for Web publishing and online ordering wizards' to 'Enabled'." Below this is a "See Also" link to a DOD STIG document. The "Reference Information" section lists various compliance standards and benchmarks.

STATUS	NAME	ACTIONS
FAILED	10.1.0.169	[More]

CAT	CCI
3.4.6, 3.4.7	CCI-000381
CM-7a.	CSF
CN-L3 7.1.3.5(c), 8.1.4.4(a)	PR.IP-1, PR.PT-3
CSF2.0 PR.PS-01	DISA_BENCHMARK Microsoft_Windows_11_ST
GDPR 32.1.b	HIPAA 164.306(a)(1)
ITSG-33 CM-7a	NIAV2 CCI-000381

3. Manual Remediation Steps

Ran gpedit.msc:

Configure the policy value for Computer Configuration >> Administrative Templates >> System >> Internet Communication Management >> Internet Communication settings >> "Turn off Internet download for Web publishing and online ordering wizards" to "Enabled".

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000105
- Status: **Passed**

Evidence:

The screenshot shows the Tenable Vulnerability Management interface. At the top, it says "Windows11DisaSTigScanBruce" under "VULNERABILITY MANAGEMENT SCANS". Below that, there are tabs for "Vulns by Plugin", "Audits" (which is selected), "Vulns by Asset", and "History". A search bar shows "WN11-CC-000105" and a result count of "1 Results". The main table has columns for "STATUS", "NAME", "FAMILY", and "COUNT". It shows one item: "Passed" (WN11-CC-000105 - Web publishing and online ordering wizards ...), Family "Windows Compliance Checks", and Count 1. On the right side, there's a summary of vulnerabilities: 0 Critical, 0 High, 0 Medium, and 0 Low. Below that, "Scan Details" show the status as "Completed" at "12/01/2025 at 4:10 PM" using the "Advanced Network Scan" template and scanner "LOCAL-SCAN-ENGINE-01". The target IP is listed as "10.10.169".

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.
- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000105

Status: **Failed**, Non-Compliant

Evidence:

Vulns by Plugin Audits Vulns by Asset History

WN11-CC-000105 1 Results

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000105 - Web publishing and online ordering wizards ...	Windows Compliance Checks	1

Scan Details

STATUS	Completed
START TIME	12/01/2025 at 4:29 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01
TARGETS	10.1.0.169

5. Remediation with PowerShell Script

Save as: Remediate-WN11-CC-000105.ps1 and run **as Administrator** utilizing PowerShell ISE:

```
# Set the value (REG_DWORD)
Set-ItemProperty -Path $regPath -Name $regName -Value $regValue -Type DWord

# Verify
$result = Get-ItemProperty -Path $regPath -Name $regName -ErrorAction Stop
"$regName" = $($result.$regName)

# Optional: force a Group Policy refresh (harmless if not GPO-managed)
& gpupdate /force | Out-Null

# Optional: restart Explorer if the UI needs the change immediately
# Stop-Process -Name explorer -Force; Start-Process explorer.exe

'NoWebServices' = 1
```

Script Used:

```
# Run as Administrator

$regPath = 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer'
$regName = 'NoWebServices'
$regValue = 1

# Ensure key exists
if (-not (Test-Path $regPath)) {
    New-Item -Path $regPath -Force | Out-Null
}

# Set the value (REG_DWORD)
Set-ItemProperty -Path $regPath -Name $regName -Value $regValue -Type DWord

# Verify
$result = Get-ItemProperty -Path $regPath -Name $regName -ErrorAction Stop
"$regName" = $($result.$regName)

# Optional: force a Group Policy refresh (harmless if not GPO-managed)
& gpupdate /force | Out-Null

# Optional: restart Explorer if the UI needs the change immediately
# Stop-Process -Name explorer -Force; Start-Process explorer.exe
```

Evidence:

The screenshot shows the Tenable Vulnerability Management interface. At the top, it displays the scan name: "Windows11DisaStigScanBruce". Below the title, there are sections for "Vulns by Plugin", "Audits", and "Vulns by Asset". The "Vulns by Plugin" section is active, showing a search bar with "WN11-CC-000105" and a results count of "1 Results". It lists one item: "WN11-CC-000105 - Web publishing and online ordering wizards ...". The status of this item is "Passed". To the right of the search bar, there are filters for Failed (0), Warning (0), and Passed (1). On the far right, there are sections for "Scan Details" (Status: Completed, Start Time: 12/01/2025 at 5:06 PM, Template: Advanced Network Scan, Scanner: LOCAL-SCAN-ENGINE-01) and "TARGETS" (IP address: 10.1.0.169).

6. Conclusion

The finding **WN11-CC-000105** 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.