

# 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. The top navigation bar includes the Tenable logo, 'Vulnerability Management', and links for 'Scans', 'Scan Details', and 'Audit Details'. A 'Quick Actions' dropdown menu is visible. The main content area displays a finding titled 'WN11-CC-000105 - Web publishing and online ordering wizards must be prevented from downloading a list of pr...'. The finding is marked as 'AUDIT FAILED'. Below the title, there are tabs for 'Overview' and 'Assets'. A search bar shows '1 Results'. A table lists the results with columns for 'STATUS', 'NAME', and 'ACTIONS'. The first row shows a 'FAILED' status for the asset '10.1.0.169'. To the right of the table, there is a 'Solution' section with instructions to 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' section with a link to a download page. A 'Reference Information' section lists various standards and benchmarks.

STATUS	NAME	ACTIONS
FAILED	10.1.0.169	

**Solution**  
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'.  
[More](#)

**See Also**  
[https://dl.dod.cyber.mil/wp-content/uploads/stigs/zlp/U\\_MS\\_Windows\\_11\\_V2R4\\_STIG.zip](https://dl.dod.cyber.mil/wp-content/uploads/stigs/zlp/U_MS_Windows_11_V2R4_STIG.zip)

**Reference Information**

800-171	800-171R3
3.4.6, 3.4.7	03.04.06a.
800-53	800-53R5
CM-7a.	CM-7a.
CAT	CCI
II	CCI-000381
CN-L3	CSF
7.1.3.5(c), 8.1.4.4(a)	PR.IP-1, PR.PT-3
CSF2.0	DISA_BENCHMARK
PR.PS-01	Microsoft_Windows_11_ST
GDPR	HIPAA
32.1.b	164.306(a)(1)
ITSG-33	NIAPV2
CM-7a	CC15a

### 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 displays the Tenable Vulnerability Management interface. At the top, the header shows 'tenable Vulnerability Management' and 'Scans > Scan Details'. The main title is 'Windows11DisaStigScanBruce'. Below this, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. A search bar contains 'WN11-CC-000105' with '1 Results' indicated. A progress bar shows '0 Failed', '0 Warning', and '1 Passed'. Below this, a table lists the scan results:

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

On the right side, there are summary statistics: 0 Critical Vulnerabilities, 0 High Vulnerabilities, 0 Medium Vulnerabilities, and 0 Low Vulnerabilities. Below these, 'Scan Details' are provided: STATUS: Completed, START TIME: 12/01/2025 at 4:10 PM, TEMPLATE: Advanced Network Scan, SCANNER: LOCAL-SCAN-ENGINE-01, and TARGETS: 10.1.0.169.

## 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:

The screenshot shows the Tenable Vulnerability Management interface. The main header displays 'tenable Vulnerability Management' and 'Scans > Scan Details'. The scan title is 'Windows11DisaStigScanBruce'. Below the title, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. The 'Audits' tab is selected, showing a search bar with 'WN11-CC-000105' and '1 Results'. A summary bar indicates 1 Failed, 0 Warning, and 0 Passed results. Below this, a table lists the audit items. The first item is 'WN11-CC-000105 - Web publishing and online ordering wizards ...' under the 'Windows Compliance Checks' family, with a count of 1 and a status of 'Failed'. On the right side, there are summary statistics for vulnerabilities: 0 Critical, 0 High, 0 Medium, and 0 Low. Below these are 'Scan Details' including Status (Completed), Start Time (12/01/2025 at 4:29 PM), Template (Advanced Network Scan), Scanner (LOCAL-SCAN-ENGINE-01), and Targets (10.1.0.169).

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

## 5. Remediation with PowerShell Script

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

The screenshot shows the Windows PowerShell ISE interface. The script is titled 'Untitled1.ps1' and contains the following code:

```
11  
12 # Set the value (REG_DWORD)  
13 Set-ItemProperty -Path $regPath -Name $regName -Value $regValue -Type Dword  
14  
15 # Verify  
16 $result = Get-ItemProperty -Path $regPath -Name $regName -ErrorAction Stop  
17 "$regName" = $($result.$regName)  
18  
19 # Optional: force a Group Policy refresh (harmless if not GPO-managed)  
20 & gpupdate /force | Out-Null  
21  
22 # Optional: restart Explorer if the UI needs the change immediately  
23 # Stop-Process -Name explorer -Force; Start-Process explorer.exe  
24  
# 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  
PS C:\Users\ThreatHunt> |
```

The script is executed successfully, as indicated by the 'Completed' status at the bottom of the console window. The taskbar at the bottom shows the system clock as 11:03 PM on 12/1/2025.

## 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 displays the Tenable Vulnerability Management interface. The main header shows 'tenable Vulnerability Management' and 'Scans > Scan Details'. The scan title is 'Windows11DisaStigScanBruce'. Below the title, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. A search bar contains 'WN11-CC-000105' and shows '1 Results'. The results are summarized in a table:

Failed	Warning	Passed
0	0	1

Below the summary, a table lists the scan results:

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

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

- CRITICAL VULNERABILITIES: 0
- HIGH VULNERABILITIES: 0
- MEDIUM VULNERABILITIES: 0
- LOW VULNERABILITIES: 0
- STATUS: Completed
- START TIME: 12/01/2025 at 5:06 PM
- TEMPLATE: Advanced Network Scan
- SCANNER: LOCAL-SCAN-ENGINE-01
- TARGETS: 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.