

STIG Implementation Report

Intern Credit Application For: Bruce Thornton

Date: 08/31/2025

STIG Finding: STIG ID: WN11-CC-000110

SRG: [SRG-OS-000095-GPOS-00049](#)

Severity: medium

CCI: CCI-000381 **Vulnerability ID:** V-253376

1. Introduction

This report documents the process of identifying, remediating, verifying, and automating the fix for a Windows 11 STIG compliance finding. The selected finding was: **STIG ID:** WN11-CC-000110 which requires that "Printing over HTTP must be prevented."

2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000110
- Status: **Fail** (non-compliant)

<https://stigaview.com/products/win11/v2r2/WN11-CC-000110/>

Printing over http must be prevented.

PowerShell Remediation

Utilizing PowerShell ISE

Registry path for the setting

```
$RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Printers"
```

```
$ValueName = "DisableHTTPPrinting"
```

```
$ValueData = 1
```

Create the key if it doesn't exist

```
if (-not (Test-Path $RegPath)) {
```

```
    New-Item -Path $RegPath -Force | Out-Null
```

```
}
```

Set the DWORD value

```
New-ItemProperty -Path $RegPath -Name $ValueName -Value $ValueData -PropertyType  
DWord -Force | Out-Null
```

Verify

```
Get-ItemProperty -Path $RegPath | Select-Object $ValueName
```

This will ensure the registry key exists and that **DisableHTTPPrinting** is set to **1**. Run
gpupdate /force

4. Verification Scan Results (After Manual Fix through Group Policy)

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000110
- Status: Passed
- Evidence:

The screenshot displays the Tenable Vulnerability Management interface. The main header shows 'tenable Vulnerability Management' and 'Scans > Scan Details'. The scan title is 'Windows11DisaStigScanAug31Bruce'. The interface is divided into three main sections: a left sidebar with navigation icons, a central results area, and a right sidebar with summary statistics and details.

Central Results Area:

- Search bar: 'WN11-CC-000110' with '1 Results'.
- Summary: 0 Failed, 0 Warning, 1 Passed.
- Table with 1 item:

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000110 - Printing over HTTP must be prevented.	Windows Compliance Checks	1

Right Sidebar Summary:

- CRITICAL VULNERABILITIES: 0
- HIGH VULNERABILITIES: 3
- MEDIUM VULNERABILITIES: 4
- LOW VULNERABILITIES: 1

Scan Details:

- STATUS: Completed
- START TIME: 08/31/2025 at 1:34 PM
- TEMPLATE: Advanced Network Scan
- SCANNER: LOCAL-SCAN-ENGINE-01
- TARGETS: 10.1.0.90

5. Reintroduction of Finding (Undo Test through Group Policy)

To demonstrate full control of the setting, the fix was undone:

- Run **gpedit.msc**.

- Navigate to:

Computer Configuration → Administrative Templates → System → Internet Communication Management → Internet Communication settings

○

- Find **“Turn off printing over HTTP”**.
- Set it to **Not Configured**.
- Click OK → run **gpupdate /force** → restart if needed.

Status: Failed

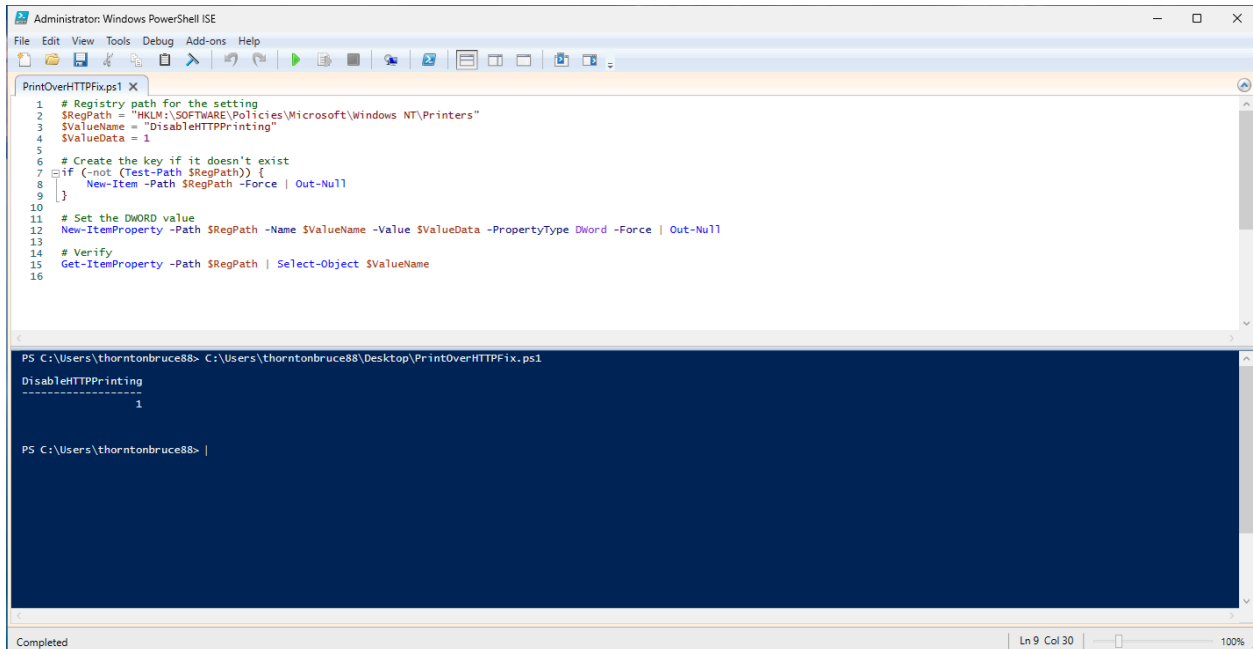
Evidence:

The screenshot displays the Tenable Vulnerability Management interface. The main header shows 'tenable Vulnerability Management' with navigation links for 'Scans' and 'Scan Details'. A search bar contains 'WN11-CC-000110' with '1 Results' indicated. Below the search bar, a summary bar shows '1 Failed', '0 Warning', and '0 Passed'. The main table lists one item: 'Failed' status, 'WN11-CC-000110 - Printing over HTTP must be prevented.', 'Windows Compliance Checks' family, and a count of '1'. On the right, a 'Scan Details' sidebar shows: 0 Critical Vulnerabilities, 3 High Vulnerabilities, 4 Medium Vulnerabilities, and 1 Low Vulnerability. It also lists scan details: Status (Completed), Start Time (08/31/2025 at 2:35 PM), Template (Advanced Network Scan), Scanner (LOCAL-SCAN-ENGINE-01), and Targets (10.1.0.90).

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000110 - Printing over HTTP must be prevented.	Windows Compliance Checks	1

6. Remediation with PowerShell Script

Ran the PowerShell script utilizing Windows PowerShell ISE.



The screenshot shows the Windows PowerShell ISE interface. The script file 'PrintOverHTTPFix.ps1' is open in the editor. The script contains the following commands:

```
1 # Registry path for the setting
2 $RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Printers"
3 $ValueName = "DisableHTTPPrinting"
4 $ValueData = 1
5
6 # Create the key if it doesn't exist
7 if (-not (Test-Path $RegPath)) {
8     New-Item -Path $RegPath -Force | Out-Null
9 }
10
11 # Set the DWORD value
12 New-ItemProperty -Path $RegPath -Name $ValueName -Value $ValueData -PropertyType DWord -Force | Out-Null
13
14 # Verify
15 Get-ItemProperty -Path $RegPath | Select-Object $ValueName
16
```

The console output shows the command being executed and the result:

```
PS C:\Users\thorntonbruce88> C:\Users\thorntonbruce88\Desktop\PrintOverHTTPFix.ps1
DisableHTTPPrinting
-----
1

PS C:\Users\thorntonbruce88> |
```

The status bar at the bottom indicates 'Completed' and 'Ln 9 Col 30'.

Restarted and ran the scan again.

Status: Passed

Evidence:

The screenshot displays the Tenable Vulnerability Management interface. The top navigation bar includes the Tenable logo, 'Vulnerability Management', and 'Scans > Scan Details'. A search bar on the left contains 'WN11-CC-000110'. The main content area shows a summary of scan results: 0 Failed, 1 Warning, and 1 Passed. Below this, a table lists the scan results. The table has columns for STATUS, NAME, FAMILY, and COUNT. The single entry is 'Passed' for 'WN11-CC-000110 - Printing over HTTP must be prevented.' under the 'Windows Compliance Checks' family, with a count of 1. On the right, a 'Scan Details' panel shows the scan status as 'Completed' on 08/31/2025 at 3:35 PM, using the 'Advanced Network Scan' template and 'LOCAL-SCAN-ENGINE-01' scanner. The target is '10.1.0.90'.

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000110 - Printing over HTTP must be prevented.	Windows Compliance Checks	1

6a. Reintroduction of Finding (Undo Test through PowerShell Script):

Utilizing PowerShell ISE

To revert (non-compliant state):

```
# Set DisableHTTPPrinting back to 0 (allow printing over HTTP)
Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Printers" -Name
"DisableHTTPPrinting" -Value 0
```

Run gpupdate /force and restart

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
RevertBackPrintOverHTTPFix.ps1 X
1 # Set DisableHTTPPrinting back to 0 (allow printing over HTTP)
2 Set-ItemProperty -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Printers" -Name "DisableHTTPPrinting" -Value 0
3

PS C:\Users\thorntonbruce88> C:\Users\thorntonbruce88\Desktop\RevertBackPrintOverHTTPFix.ps1
PS C:\Users\thorntonbruce88> C:\Users\thorntonbruce88\Desktop\RevertBackPrintOverHTTPFix.ps1
PS C:\Users\thorntonbruce88> gpupdate /Force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\thorntonbruce88> |
```

Completed Ln 17 Col 30 100%

Restart and scan again for verification.

Status: Failed

Evidence:

tenable Vulnerability Management | Scans > Scan Details

Windows11DisaStigScanAug31Bruce

VULNERABILITY MANAGEMENT SCANS

Vulns by Plugin Audits Vulns by Asset History

WN11-CC-000110 1 Results

1 Failed 0 Warning 0 Passed

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000110 - Printing over HTTP must be prevented.	Windows Compliance Checks	1

1 Item 1 to 1 of 1 Page 1 of 1

Quick Actions

0 CRITICAL VULNERABILITIES 3 HIGH VULNERABILITIES 4 MEDIUM VULNERABILITIES 1 LOW VULNERABILITIES

Scan Details

STATUS Completed

START TIME 08/31/2025 at 4:30 PM

TEMPLATE Advanced Network Scan

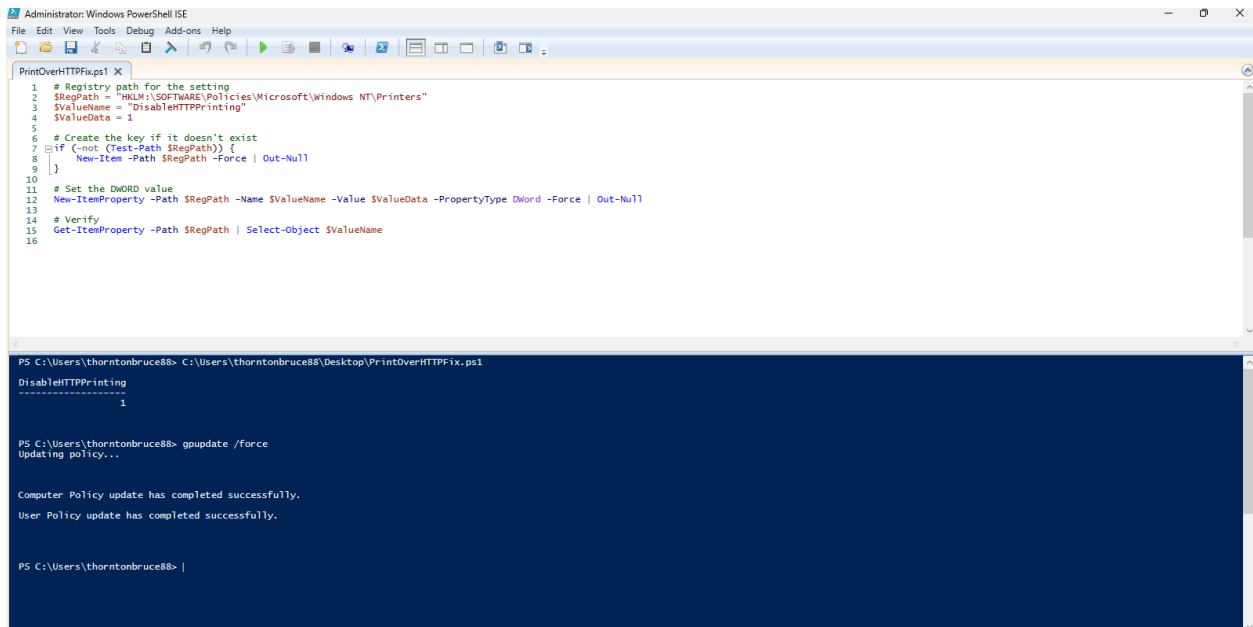
SCANNER LOCAL-SCAN-ENGINE-01

TARGETS 10.1.0.90

6b. Remediation with PowerShell Script

Ran the PowerShell script utilizing Windows PowerShell ISE.

Final Remediation.



The screenshot shows the Windows PowerShell ISE interface. The top pane displays a PowerShell script named 'PrintOverHTTPFix.ps1'. The script sets a registry path, creates a new registry value 'DisableHTTPPrinting' with a value of 1, and verifies the change. The bottom pane shows the execution output, which includes the command 'gupdate /force' and messages indicating that computer and user policy updates have completed successfully.

```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help

PrintOverHTTPFix.ps1 X
1 # Registry path for the setting
2 $RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Printers"
3 $ValueName = "DisableHTTPPrinting"
4 $ValueData = 1
5
6 # Create the key if it doesn't exist
7 if (not (Test-Path $RegPath)) {
8     New-Item -Path $RegPath -force | Out-Null
9 }
10
11 # Set the DWORD value
12 New-ItemProperty -Path $RegPath -Name $ValueName -Value $ValueData -PropertyType DWORD -Force | Out-Null
13
14 # Verify
15 Get-ItemProperty -Path $RegPath | Select-Object $ValueName
16

PS C:\Users\thorntonbruce88> C:\Users\thorntonbruce88\Desktop\PrintOverHTTPFix.ps1
DisableHTTPPrinting
-----
1

PS C:\Users\thorntonbruce88> gupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.

PS C:\Users\thorntonbruce88> |
```

Also ran gpupdate /force, and restarted.

Status: Passed

Evidence:

tenable Vulnerability Management | Scans > Scan Details

Quick Actions

Windows11DisaStigScanAug31Bruce

Vulns by Plugin Audits Vulns by Asset History

WN11-CC-000110 1 Results

0 Failed 1 Warning 1 Passed

1 Item

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000110 - Printing over HTTP must be prevented.	Windows Compliance Checks	1

1 to 1 of 1 Page 1 of 1

CRITICAL VULNERABILITIES 0

HIGH VULNERABILITIES 3

MEDIUM VULNERABILITIES 4

LOW VULNERABILITIES 1

Scan Details

STATUS Completed

START TIME 08/31/2025 at 5:39 PM

TEMPLATE Advanced Network Scan

SCANNER LOCAL-SCAN-ENGINE-01

TARGETS 10.1.0.90

7. Conclusion

The finding **WN11-CC-000110** 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 automation.

