

STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
Date: 09/29/2025
STIG Finding: STIG ID: WN11-CC-000326
 - **SRG:** [SRG-OS-000042-GPOS-00020](#)
Severity: medium
Vulnerability ID: V-253414 **CCI:** CCI-000135
-

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-000326 "PowerShell script block logging must be enabled on Windows 11."

2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000326
- Status: **Fail** (non-compliant)

 **Evidence:** First identified the STIG:

<https://stigaview.com/products/win11/v2r3/WN11-CC-000326/>

Initial scan result:

The screenshot displays the Tenable Vulnerability Management interface. At the top, the 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 'Win11DisaStigBruceSept29' and a search bar containing 'WN11-CC-000326'. Below the header, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. The 'Audits' tab is active, showing a summary of results: 1 Failed, 0 Warning, and 0 Passed. A table below this summary lists the findings. The table has columns for 'STATUS', 'NAME', 'FAMILY', and 'COUNT'. One finding is listed with a status of 'Failed', the name 'WN11-CC-000326 - PowerShell script block logging must be enabl...', the family 'Windows Compliance Checks', and a count of 1. On the right side of the interface, there is a summary of vulnerability counts: 0 Critical, 0 High, 0 Medium, and 0 Low vulnerabilities. Below this, the 'Scan Details' section shows the status as 'Completed', the start time as '09/28/2025 at 8:52 PM', the template as 'Advanced Network Scan', the scanner as 'LOCAL-SCAN-ENGINE-01', and the target as '10.1.0.94'.

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000326 - PowerShell script block logging must be enabl...	Windows Compliance Checks	1

3. Manual Remediation Steps

Run "gpedit.msc"

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows PowerShell >> "Turn on PowerShell Script Block Logging" to "Enabled".

Run "gpupdate /force" and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000326
- Status: Passed

Evidence:

tenable Vulnerability Management | Scans > Scan Details

Win11DisaStigBruceSept29

VULNERABILITY MANAGEMENT SCANS

Vulns by Plugin Audits Vulns by Asset History

WN11-CC-000326 1 Results

0 Failed 0 Warning 1 Passed

1 Item

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000326 - PowerShell script block logging must be enabl...	Windows Compliance Checks	1

Scan Details

STATUS Completed

START TIME 09/28/2025 at 9:31 PM

TEMPLATE Advanced Network Scan

SCANNER LOCAL-SCAN-ENGINE-01

TARGETS 10.1.0.94

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:

tenable Vulnerability Management | Scans > Scan Details

Win11DisaStigBruceSept29

VULNERABILITY MANAGEMENT SCANS

Vulns by Plugin Audits Vulns by Asset History

WN11-CC-000326 1 Results

1 Failed 0 Warning 0 Passed

1 Item

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000326 - PowerShell script block logging must be enabl...	Windows Compliance Checks	1

Scan Details

STATUS Completed

START TIME 09/28/2025 at 10:05 PM

TEMPLATE Advanced Network Scan

SCANNER LOCAL-SCAN-ENGINE-01

TARGETS 10.1.0.94

5. Remediation with PowerShell Script

We opened PowerShell ISE within the Virtual Machine and ran this script:

```
<#
.SYNOPSIS
    Remediates STIG ID WN11-CC-000326:
    Enables PowerShell Script Block Logging on Windows 11.

.DESCRIPTION
    This script creates or updates the registry key required
    to enforce script block logging. Must be run with Administrator privileges.
#>

# Ensure running as Administrator
If (-NOT ([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole(
    [Security.Principal.WindowsBuiltinRole] "Administrator")) {
    Write-Error "You must run this script as Administrator."
    Exit 1
}

# Define registry path and value
$RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging"
$RegName = "EnableScriptBlockLogging"
$RegValue = 1

# Create registry path if missing
If (-Not (Test-Path $RegPath)) {
    New-Item -Path $RegPath -Force | Out-Null
    Write-Output "Created registry path: $RegPath"
}

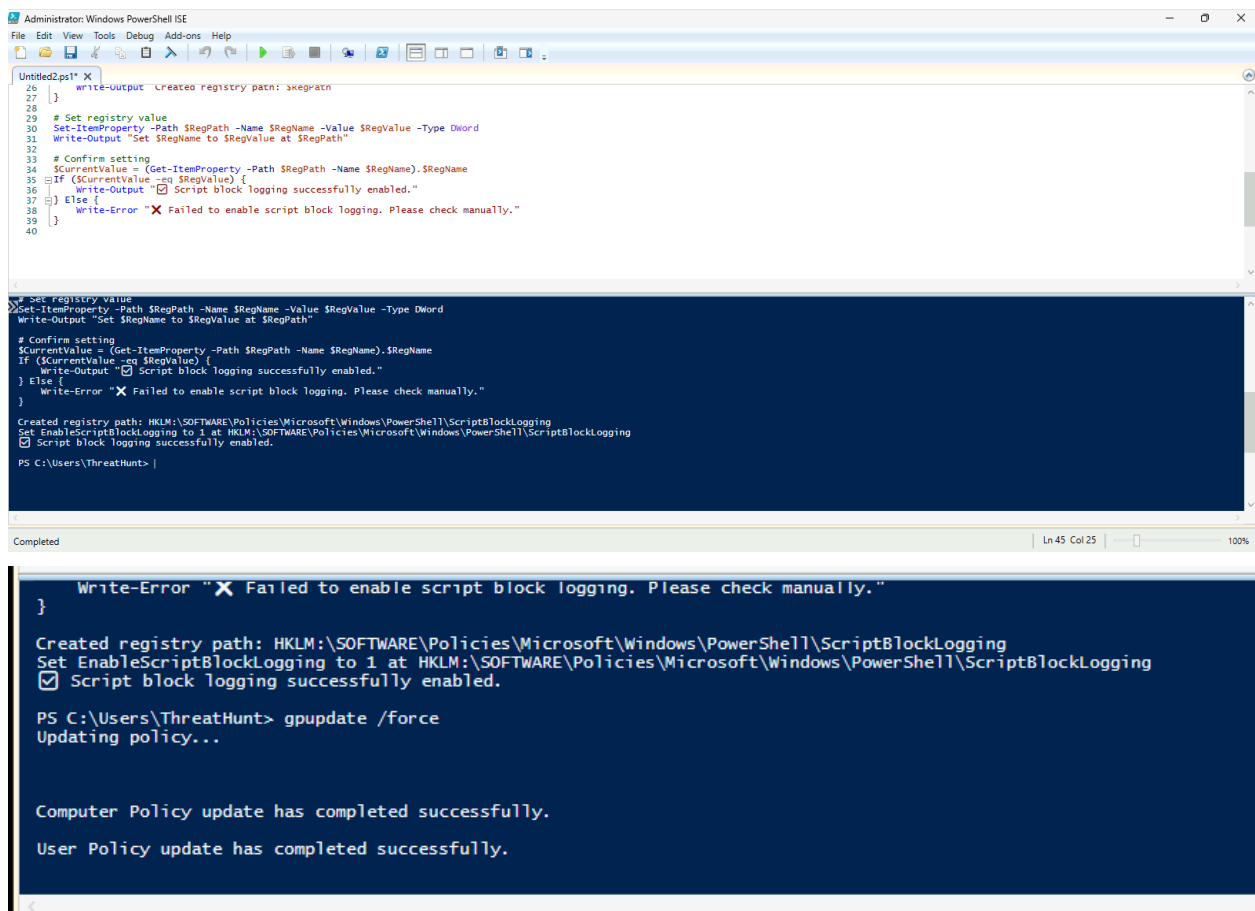
# Set registry value
Set-ItemProperty -Path $RegPath -Name $RegName -Value $RegValue -Type DWord
Write-Output "Set $RegName to $RegValue at $RegPath"

# Confirm setting
$CurrentValue = (Get-ItemProperty -Path $RegPath -Name $RegName).$RegName
If ($CurrentValue -eq $RegValue) {
    Write-Output "✅ Script block logging successfully enabled."
} Else {
    Write-Error "❌ Failed to enable script block logging. Please check manually."
}
```

How it works:

1. Checks if you're running as **Administrator**.
2. Creates the registry path if missing.
3. Sets **EnableScriptBlockLogging** = 1.
4. Confirms and outputs success/failure.

This can be saved as: **Remediate-WN11-CC-000326.ps1** and run it in **PowerShell ISE (Run as Admin)**.



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled2.ps1 X
26 }
27 Write-Output "Created registry path: $RegPath"
28 }
29 # Set registry value
30 Set-ItemProperty -Path $RegPath -Name $RegName -Value $RegValue -Type DWord
31 Write-Output "Set $RegName to $RegValue at $RegPath"
32
33 # Confirm setting
34 $CurrentValue = (Get-ItemProperty -Path $RegPath -Name $RegName).$RegName
35 If ($CurrentValue -eq $RegValue) {
36 Write-Output "Script block logging successfully enabled."
37 } Else {
38 Write-Error "X Failed to enable script block logging. Please check manually."
39 }
40
# Set registry value
Set-ItemProperty -Path $RegPath -Name $RegName -Value $RegValue -Type DWord
Write-Output "Set $RegName to $RegValue at $RegPath"

# Confirm setting
$CurrentValue = (Get-ItemProperty -Path $RegPath -Name $RegName).$RegName
If ($CurrentValue -eq $RegValue) {
Write-Output "Script block logging successfully enabled."
} Else {
Write-Error "X Failed to enable script block logging. Please check manually."
}

Created registry path: HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging
Set EnableScriptBlockLogging to 1 at HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging
Script block logging successfully enabled.
PS C:\Users\ThreatHunt>

Completed Ln 45 Col 25 100%

} Write-Error "X Failed to enable script block logging. Please check manually."

Created registry path: HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging
Set EnableScriptBlockLogging to 1 at HKLM:\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging
Script block logging successfully enabled.

PS C:\Users\ThreatHunt> gpupdate /force
Updating policy...

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

Ran gpupdate /force and then restart.

Status: Passed

Evidence:

The screenshot displays the Tenable Vulnerability Management interface. At the top, the navigation bar includes the Tenable logo, 'Vulnerability Management', and a breadcrumb trail 'Scans > Scan Details'. On the right, there are 'Quick Actions' and a user profile icon labeled 'BR'. The main header shows the scan name 'Win11DisaStigBruceSept29' with a search icon and buttons for 'Export', 'Edit', and 'Trash'. Below the header, there are tabs for 'Vulns by Plugin', 'Audits' (selected), 'Vulns by Asset', and 'History'. A search bar contains 'WN11-CC-000326' and shows '1 Results'. A summary bar indicates '0 Failed', '0 Warning', and '1 Passed'. A table lists one item: 'Passed', 'WN11-CC-000326 - PowerShell script block logging must be enabl...', 'Windows Compliance Checks', and '1'. On the right, a 'Scan Details' panel shows vulnerability counts (0 Critical, 0 High, 0 Medium, 0 Low) and scan metadata: Status (Completed), Start Time (09/28/2025 at 10:34 PM), Template (Advanced Network Scan), Scanner (LOCAL-SCAN-ENGINE-01), and Targets (10.1.0.94).

6. Conclusion

The finding **WN11-CC-000326** 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.