

# STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton

**Date:** 09/01/2025

**STIG Finding:** STIG ID: WN11-CC-000285

- **SRG:** [SRG-OS-000250-GPOS-00093](#)

**Severity:** Medium

**Vulnerability ID:**V-253405 **CCI:** CCI-001453

---

## 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-000285  
The Remote Desktop Session Host must require secure RPC communications.

---

## 2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000285
- Status: **Fail** (non-compliant)

 **Evidence:** First identified the STIG:

<https://stigaview.com/products/win11/v1r6/WN11-CC-000285/>

Along with initial scan results:

tenable Vulnerability Management | Scans > Scan Details > Audit Details

Quick Actions

### WN11-CC-000285 - The Remote Desktop Session Host must require secure RPC communications.

AUDIT **FAILED**

Overview Assets

Search 1 Results

STATUS	NAME	ACTIONS
FAILED	10.1.0.84	

1 Result 1 to 1 of 1 Page 1 of 1

**Solution**

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security . . .  
[More](#)

**See Also**

[https://dl.dod.cyber.mil/wp-content/uploads/stigs/zlp/U\\_MS\\_Windows\\_11\\_V2R3\\_STIG.zip](https://dl.dod.cyber.mil/wp-content/uploads/stigs/zlp/U_MS_Windows_11_V2R3_STIG.zip)

**Reference Information**

800-171 3.1.13	800-171R3 03.13.08
800-53 AC-17(2)	800-53RS AC-17(2)
CAT II	CCI CCI-001453
CN-L3 7.1.2.7(g), 7.1.3.1(d), 8.1.4.1(c)	CSF PR.AC-3, PR.PT-4
CSF2.0 PR.AA-05	DISA_BENCHMARK Microsoft_Windows_11_ST
GDPR 32.1.b	HIPAA 164.306(a)(1), 164.312(a) (1)
ISO-27001-2022	ISO/IEC-27001

### 3. Manual Remediation Steps

- Performed the following changes using Group Policy:
- Open **Group Policy Management** ([gpedit.msc](#)).
- Navigate to: Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Security
- Locate and **enable** the policy: Require secure RPC communication
- Run [gpupdate /force](#) to apply the policy.
- Scan: Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)

Status: Passed

Evidence:

tenable Vulnerability Management | Scans > Scan Details

Quick Actions ?

### Windows11DisaStigScanSept1Bruce

VULNERABILITY MANAGEMENT SCANS

[Export] [Edit] [Trash]

Vulns by Plugin Audits Vulns by Asset History

WN11-CC-000285 1 Results

0 Failed 1 Warning 1 Passed

1 item 1 to 1 of 1 Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000285 - The Remote Desktop Session Host must requi...	Windows Compliance Checks	1

**Scan Details**

STATUS: Completed

START TIME: 09/01/2025 at 3:28 PM

TEMPLATE: Advanced Network Scan

SCANNER: LOCAL-SCAN-ENGINE-01

TARGETS: 10.1.0.84

## 5. Reintroduction of Finding (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 “Not Configured.”
- Ran `gpupdate /force` and rescanned.

Status: Failed, Non-Compliant

Evidence:

tenable Vulnerability Management | Scans > Scan Details

Windows11DisaStigScanSept1Bruce

VULNERABILITY MANAGEMENT SCANS

Vulns by Plugin Audits Vulns by Asset History

WN11-CC-000285 1 Results

1 Failed 1 Warning 1 Passed

1 Item

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000285 - The Remote Desktop Session Host must requi...	Windows Compliance Checks	1

1 to 1 of 1 Page 1 of 1

CRITICAL VULNERABILITIES 0

HIGH VULNERABILITIES 0

MEDIUM VULNERABILITIES 0

LOW VULNERABILITIES 0

Scan Details

STATUS Completed

START TIME 09/01/2025 at 3:48 PM

TEMPLATE Advanced Network Scan

SCANNER LOCAL-SCAN-ENGINE-01

TARGETS 10.1.0.84

## 6. Remediation

### PowerShell Remediation

Utilizing PowerShell ISE

To automate the remediation process, you can use the following PowerShell script:

# Define registry path and value

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

```
$ValueName = "fEncryptRPCTraffic"
```

```
$ValueData = 1
```

# Create registry key if it doesn't exist

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

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

```
}
```

# Set the registry value

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

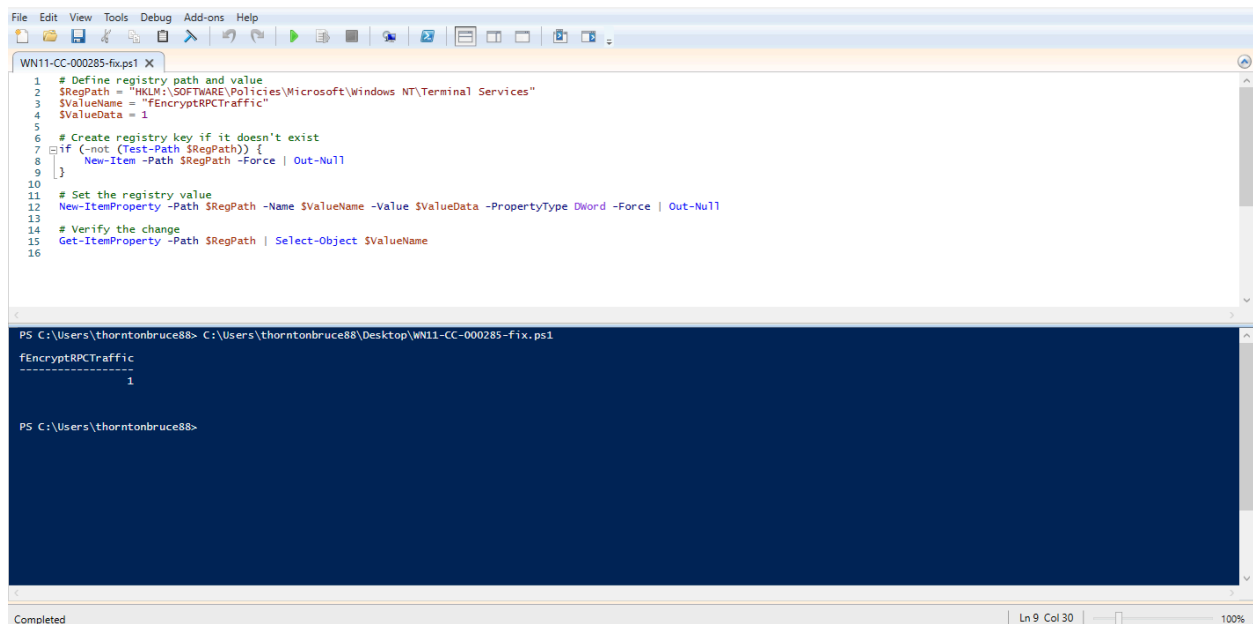
# Verify the change

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

### Explanation:

- The script checks if the specified registry path exists; if not, it creates it.
- It then sets the `fEncryptRPCTraffic` value to `1`, ensuring secure RPC communication.
- Finally, it verifies that the change has been applied correctly.

After running this script and scanning again,



The screenshot shows a PowerShell script editor window titled "WN11-CC-000285-fix.ps1". The script contains the following code:

```
1 # Define registry path and value  
2 $RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services"  
3 $ValueName = "fEncryptRPCTraffic"  
4 $ValueData = 1  
5  
6 # Create registry 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 registry value  
12 New-ItemProperty -Path $RegPath -Name $ValueName -Value $ValueData -PropertyType DWord -Force | Out-Null  
13  
14 # Verify the change  
15 Get-ItemProperty -Path $RegPath | Select-Object $ValueName  
16
```

Below the script editor is a PowerShell console window showing the execution of the script. The prompt is "PS C:\Users\thorntonbruce88> C:\Users\thorntonbruce88\Desktop\WN11-CC-000285-fix.ps1". The output shows the registry value "fEncryptRPCTraffic" being set to "1".

```
PS C:\Users\thorntonbruce88> C:\Users\thorntonbruce88\Desktop\WN11-CC-000285-fix.ps1  
fEncryptRPCTraffic  
1  
PS C:\Users\thorntonbruce88>
```

The console window status bar at the bottom indicates "Completed" and "Ln 9 Col 30".

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 'Windows11DisaStigScanSept1Bruce' with options to 'Export', 'Edit', or 'Trash'. Below this, tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History' are present, with 'Audits' selected. A search bar contains 'WN11-CC-000285' and indicates '1 Results'. A summary bar shows '0 Failed', '0 Warning', and '1 Passed'. The main table lists one item: 'WN11-CC-000285 - The Remote Desktop Session Host must requ...' with a status of 'Passed', family of 'Windows Compliance Checks', and a count of '1'. The right sidebar provides a summary of vulnerabilities (0 Critical, 0 High, 0 Medium, 0 Low) and scan details including status (Completed), start time (09/01/2025 at 4:08 PM), template (Advanced Network Scan), scanner (LOCAL-SCAN-ENGINE-01), and targets (10.1.0.84).

## 7. Conclusion

The finding **WN11-CC-000285** 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.

