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.

---

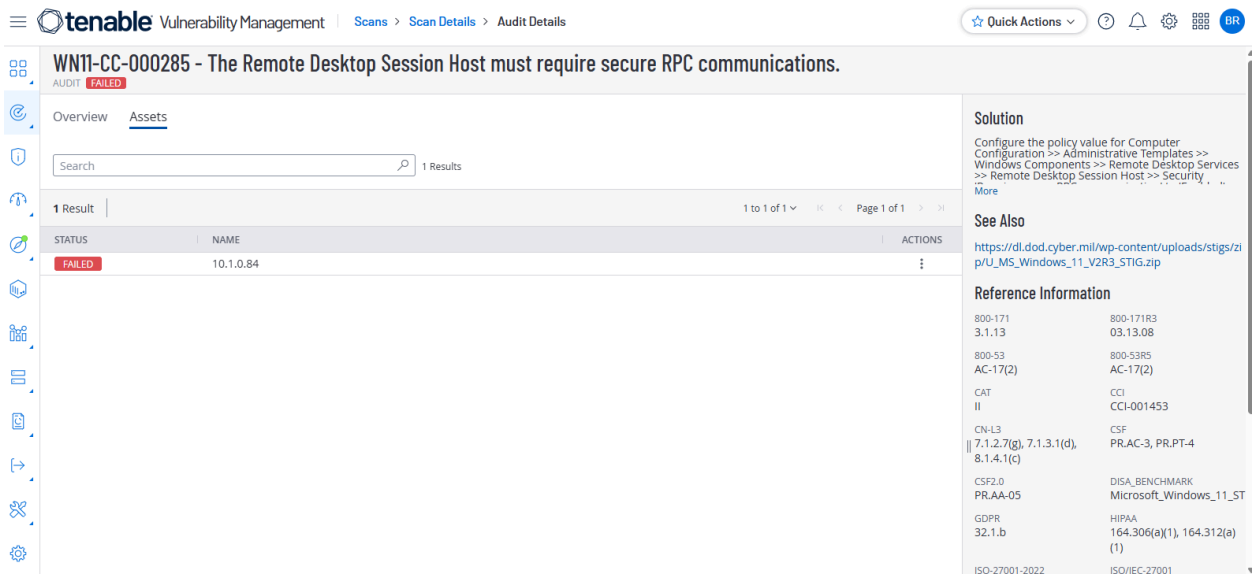
2. Initial Scan Results

- 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:



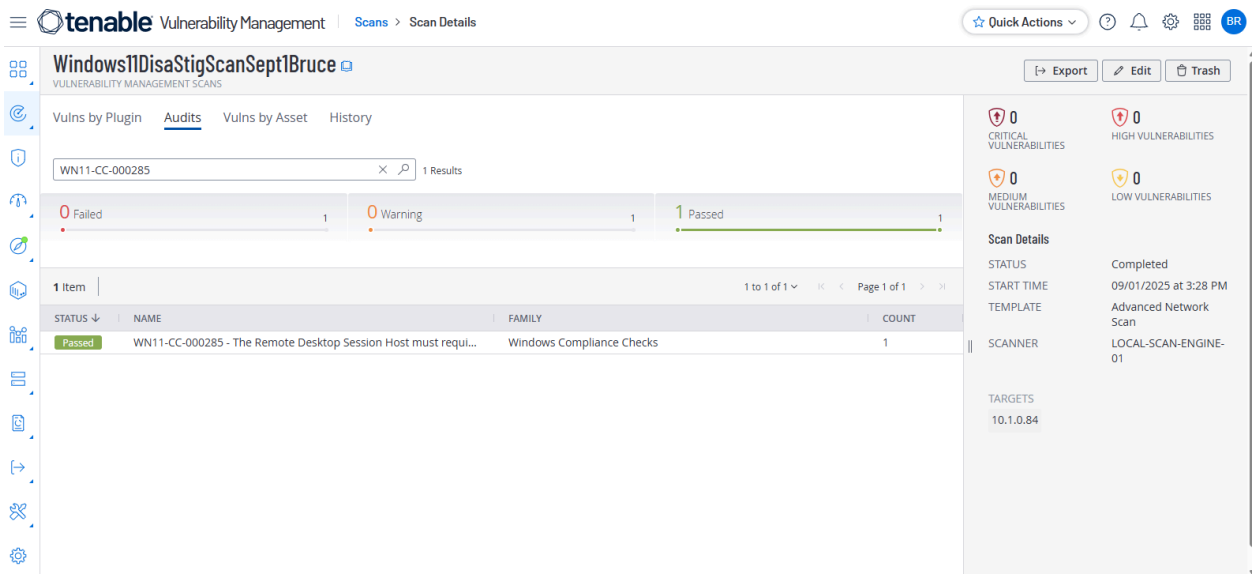
---

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:



---

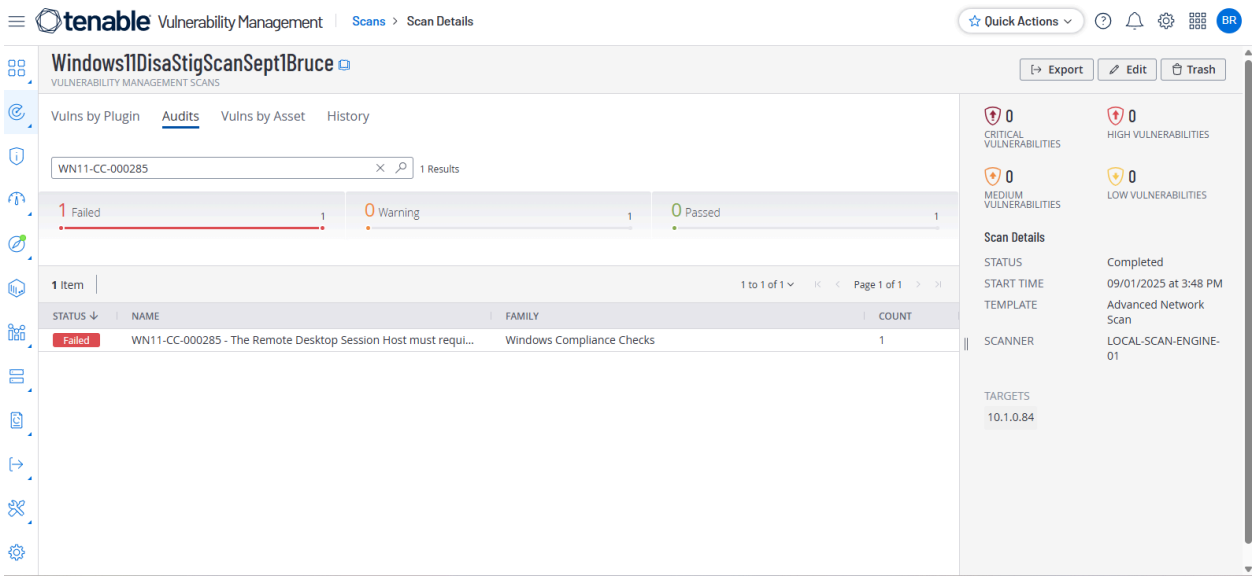
5. Reintroduction of Finding (Undo Test)

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:



---

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

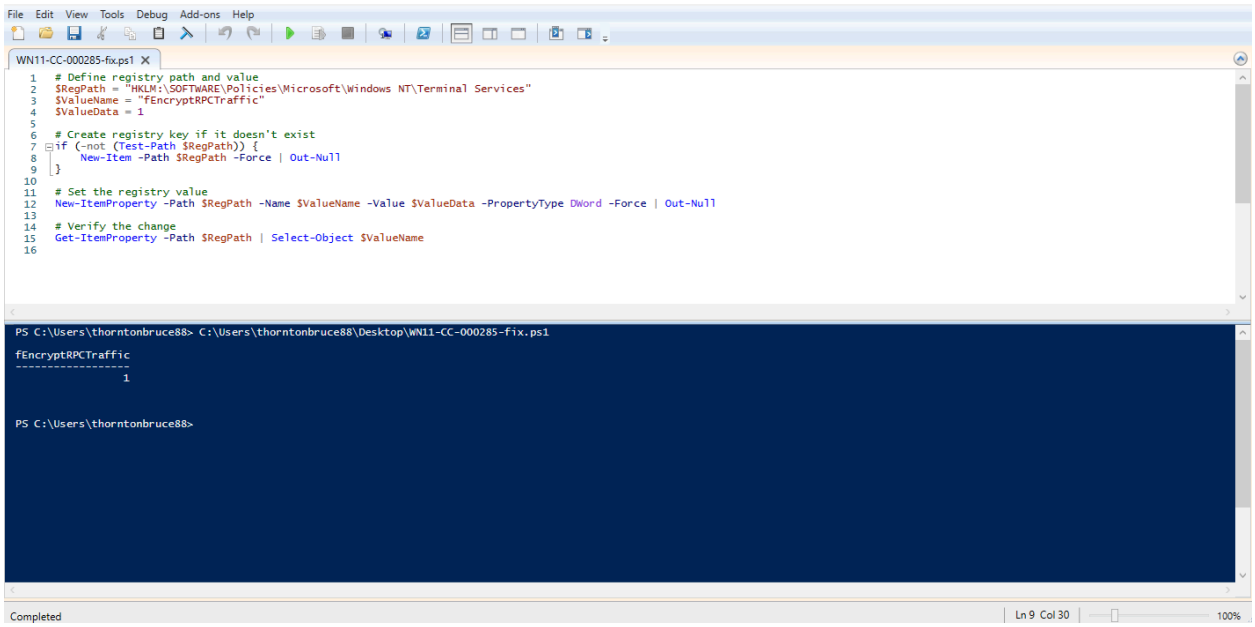
Verify the change

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

Explanation:

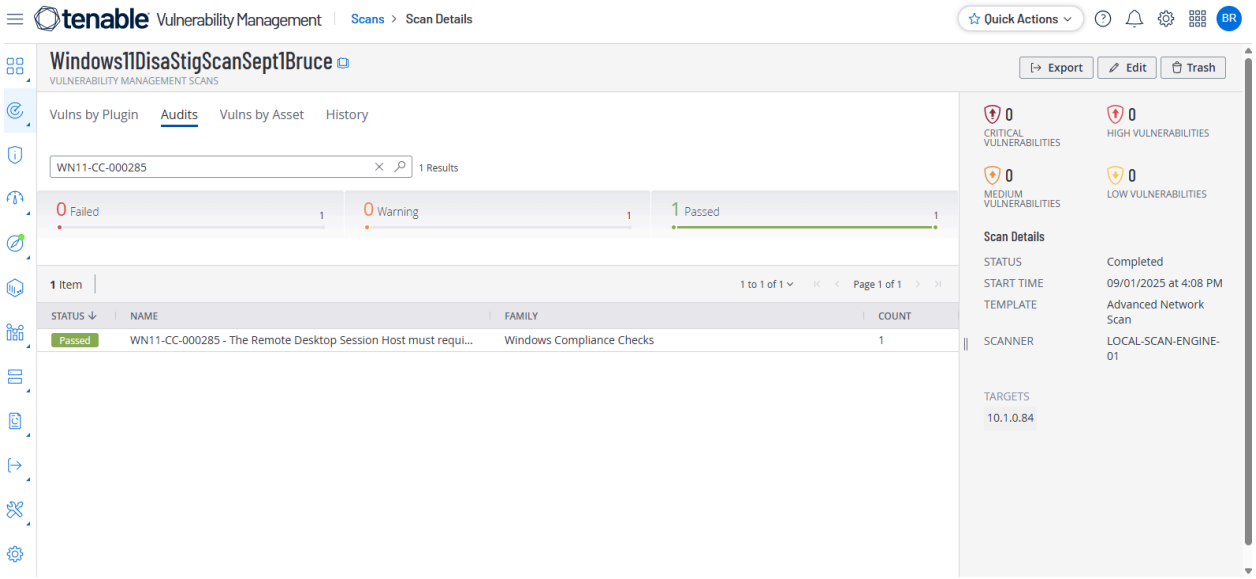
- The script checks if the specified registry path exists; if not, it creates it.
- It then sets the `fEncryptRPCTraffic` value to `1`, ensuring secure RPC communication.
- Finally, it verifies that the change has been applied correctly.

After running this script and scanning again,



Status: Passed

Evidence:



---

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.