STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
  Date: 09/06/2025
  STIG Finding: STIG ID: WN11-CC-000350
- **SRG:** SRG-OS-000394-GPOS-00174
  Severity: Medium
  Vulnerability ID:V-253419 **CCI:** CCI-003123

---

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-00035 “The Windows Remote Management (WinRM) service must not allow unencrypted traffic.”

---

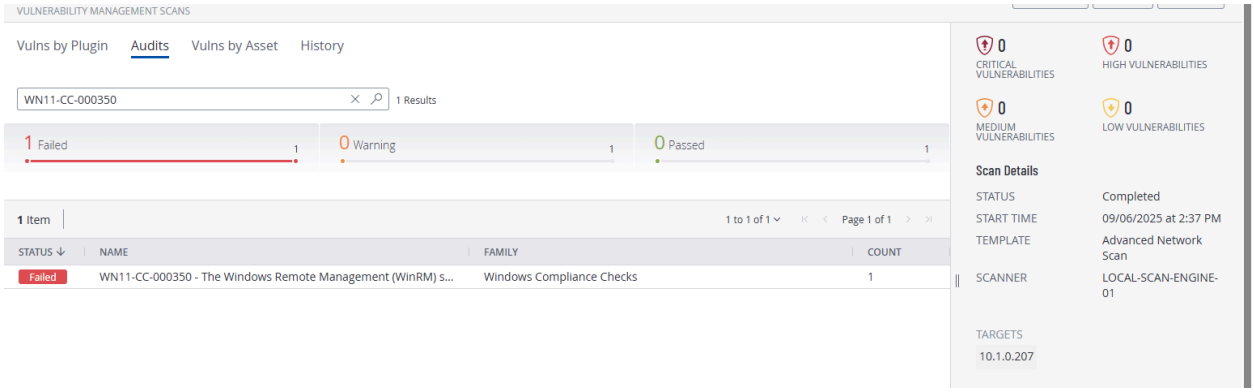
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-00035
- Status: **Fail** (non-compliant)

📎 **Evidence:** First identified the STIG:

https://stigaview.com/products/win11/v2r3/WN11-CC-000350/

Along with initial scan results:



---

3. Manual Remediation Steps

Performed the following manual changes through “gpedit.msc.”

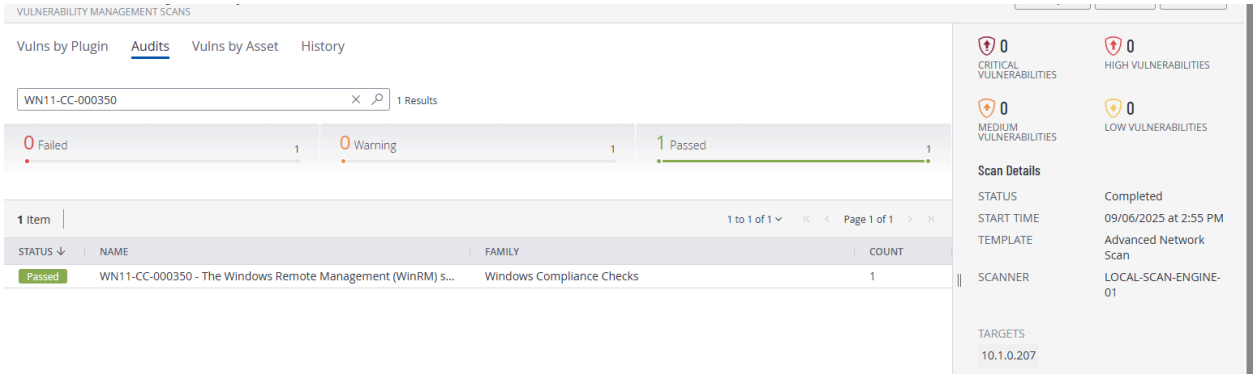
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows Remote Management (WinRM) >> WinRM Service >> "Allow unencrypted traffic" to "Disabled".

Ran “gpupdate /force” and then restarted.

Launched another scan:

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-00035
- Status: Passed

Evidence:



---

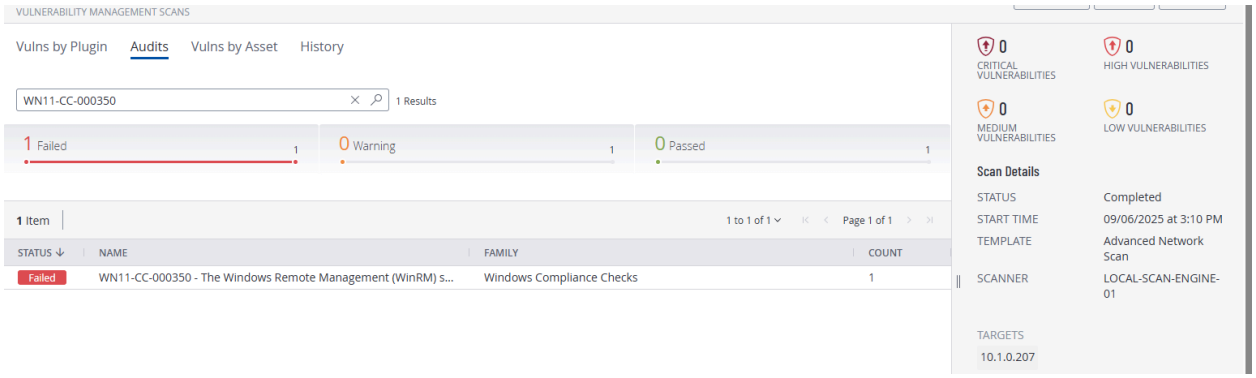
4. Reintroduction of Finding (Undo Test)

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:



---

5. Remediation

PowerShell Remediation

Utilizing PowerShell ISE

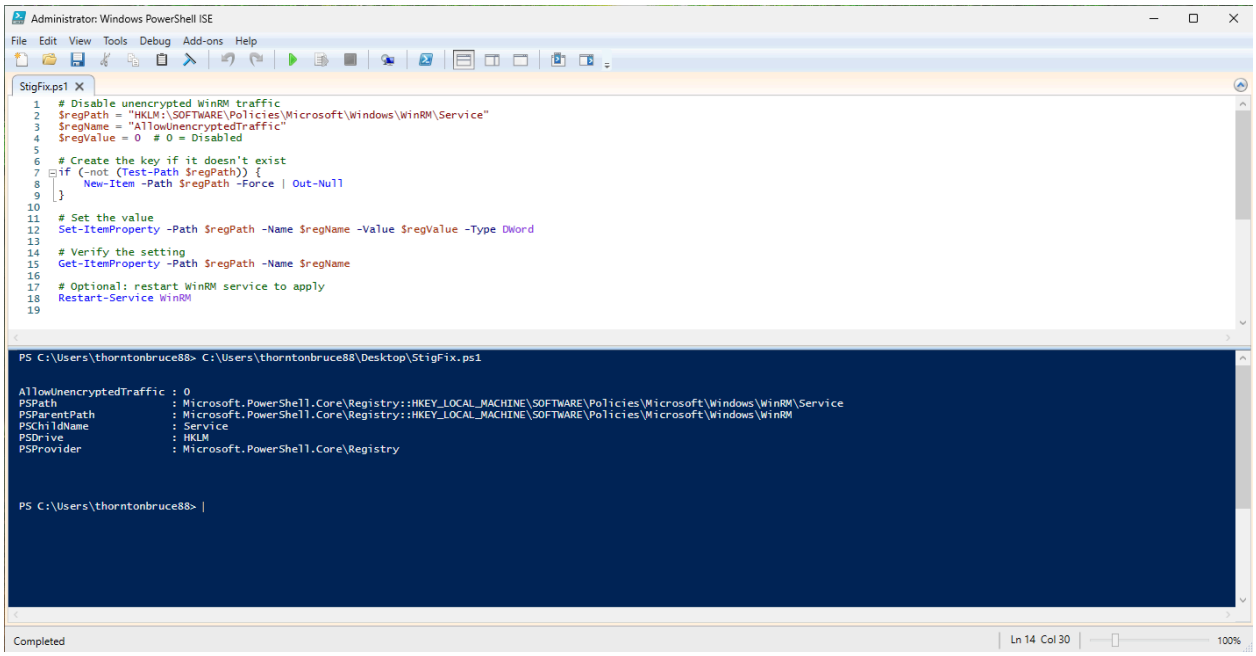
To automate the remediation process, you can use the following PowerShell script:

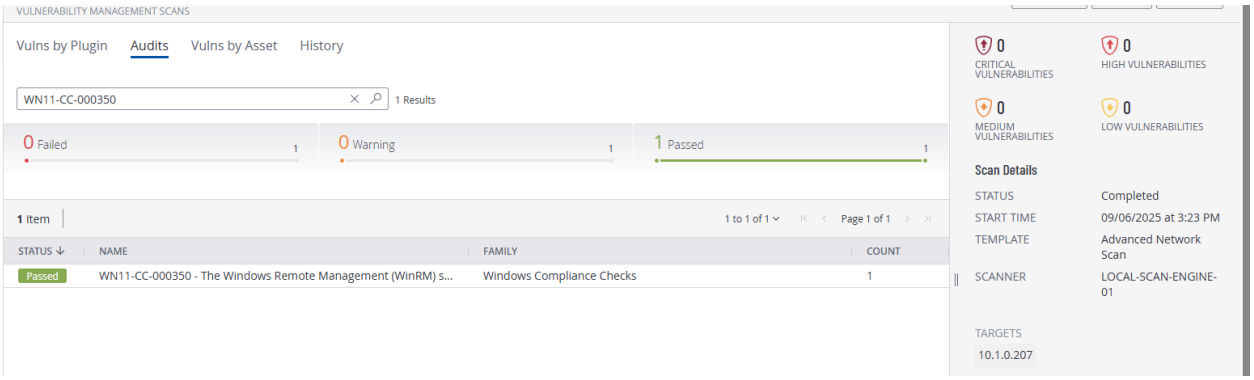
```
# Disable unencrypted WinRM traffic
$regPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service"
$regName = "AllowUnencryptedTraffic"
$regValue = 0  # 0 = Disabled

# Create the key if it doesn't exist
if (-not (Test-Path $regPath)) {
    New-Item -Path $regPath -Force | Out-Null
}

# Set the value
Set-ItemProperty -Path $regPath -Name $regName -Value $regValue -Type DWord

# Verify the setting
Get-ItemProperty -Path $regPath -Name $regName

# Optional: restart WinRM service to apply
Restart-Service WinRM
```

After running this script and scanning again,

Status: Passed

Evidence:





---

6. Conclusion

The finding **WN11-CC-00035** 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 manually and remediated through PowerShell automation, and validated with a third scan.

This demonstrates the ability to manage Windows STIG compliance both manually and through automation with PowerShell.