STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
  Date: 09/11/2025
  STIG Finding: STIG ID: WN11-00-000032
- **SRG:** SRG-OS-000121-GPOS-00062
  Severity: medium
  Vulnerability ID: V-253261 **CCI:** CCI-000804

---

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-000310 “Windows 11 systems must use a BitLocker PIN with a minimum length of six digits for pre-boot authentication”

---

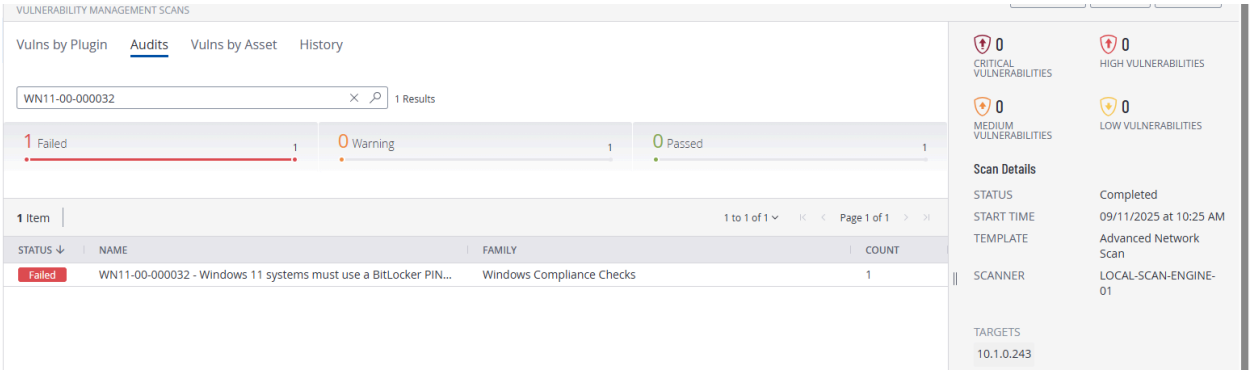
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-00-000032
- Status: **Fail** (non-compliant)

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

https://stigaview.com/products/win11/v2r2/WN11-00-000032/

Initial scan result:



---

3. Manual Remediation Steps

Run "gpedit.msc".

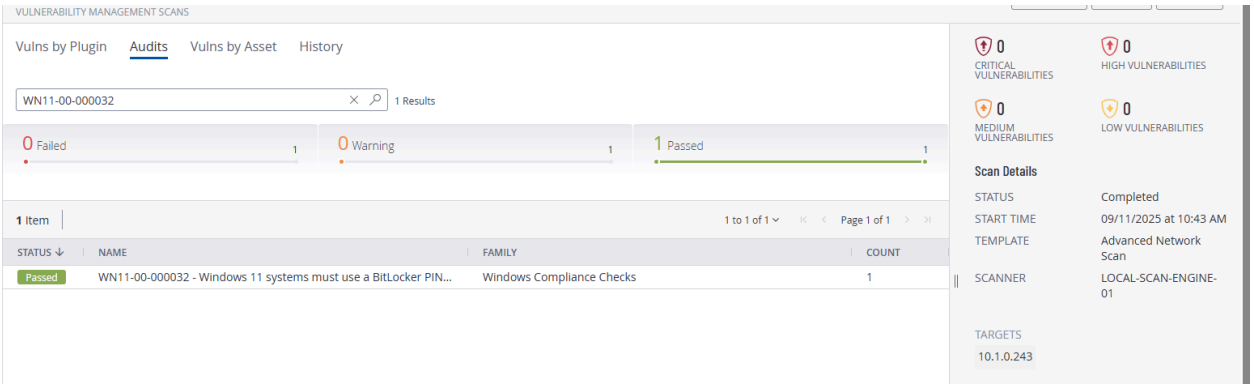
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> BitLocker Drive Encryption >> Operating System Drives "Configure minimum PIN length for startup" to "Enabled" with "Minimum characters:" set to "6" or greater.

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-00-000032
- Status: Passed

Evidence:



4. Reintroduction of Finding (Manually Undo Test)

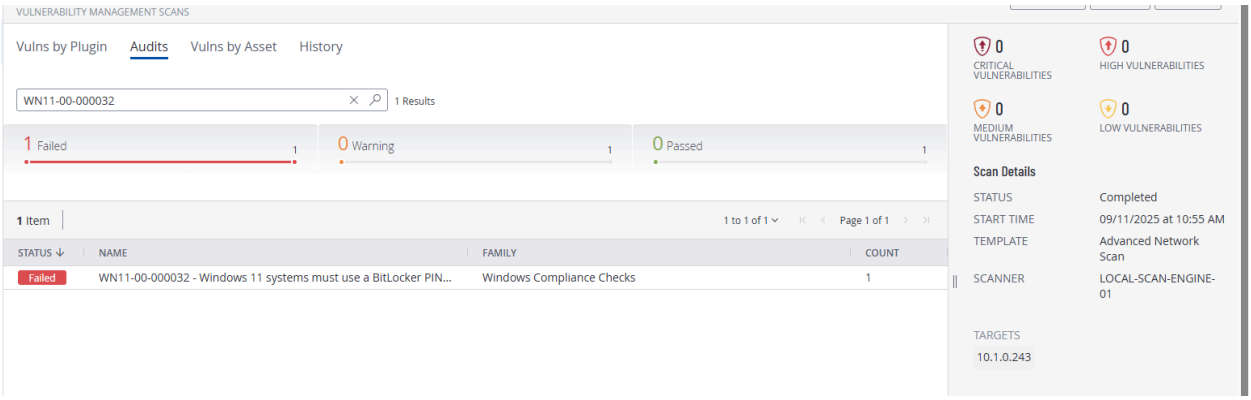
To demonstrate full control of the setting, the fix was undone:

- 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:



5. Manual Remediation Steps

Run "gpedit.msc".

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> BitLocker Drive Encryption >> Operating System Drives "Configure minimum PIN length for startup" to "Enabled" with "Minimum characters:" set to "6" or greater.

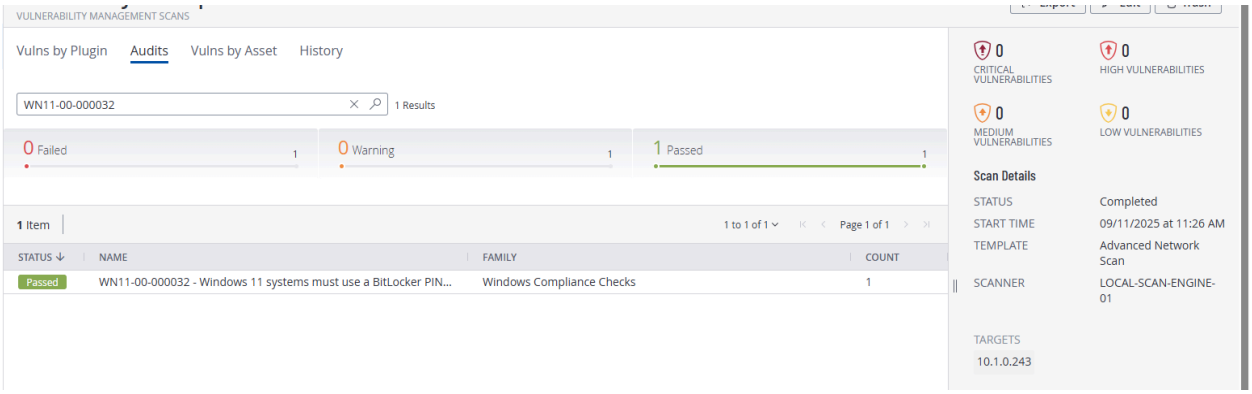
Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)

- Finding ID: WN11-00-000032
- Status: Passed

Evidence:



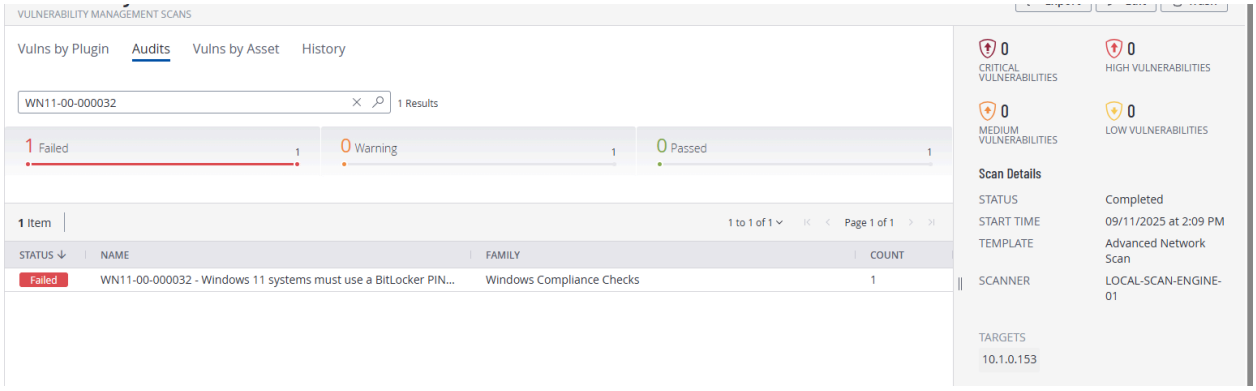
---

6. Test Remediation with PowerShell Script

Created a new Virtual Machine.
Scanned,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-00-000032
- Status: Failed

Evidence:



Remediation Utilizing PowerShell ISE:

```
# WN11-00-000032 - Enforce BitLocker PIN with minimum 6 digits

$regPath = "HKLM:\SOFTWARE\Policies\Microsoft\FVE"

# Ensure the policy path exists
if (-not (Test-Path $regPath)) {
    New-Item -Path $regPath -Force | Out-Null
}

# Require TPM + PIN
Set-ItemProperty -Path $regPath -Name "UseTPMPIN" -Value 1 -Type DWord

# Minimum PIN length (set to 6 per STIG)
Set-ItemProperty -Path $regPath -Name "MinimumPIN" -Value 6 -Type DWord

Write-Output "BitLocker TPM+PIN requirement and minimum PIN length set to 6."
```

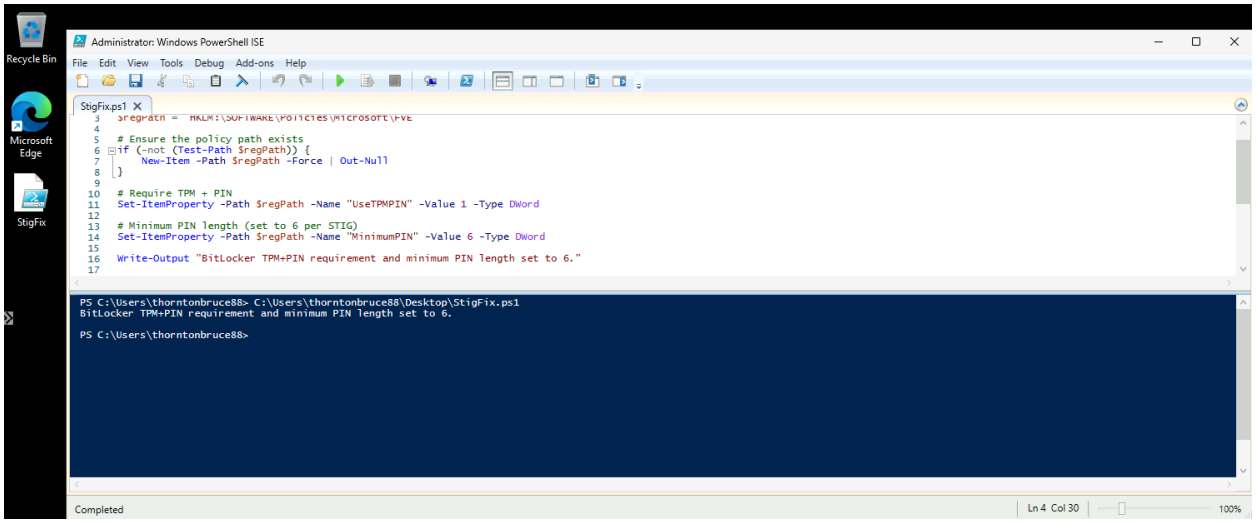
Notes:

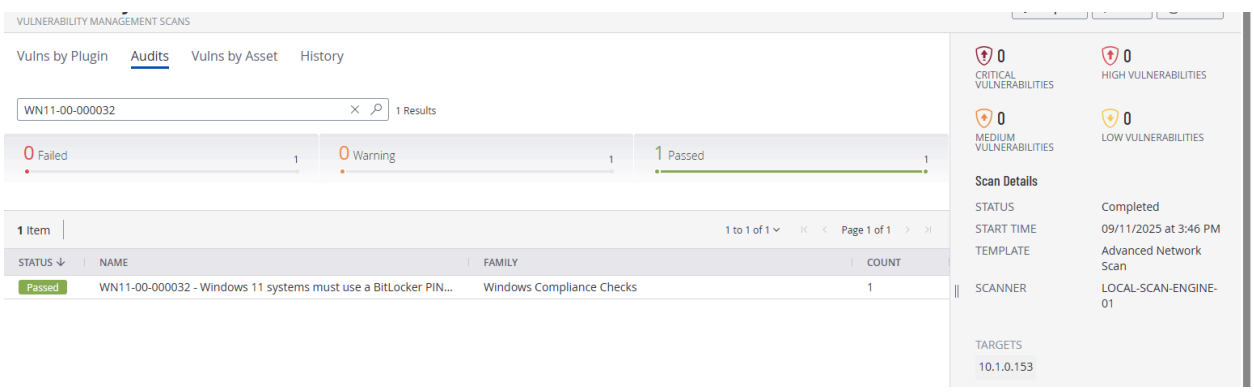
- You'll need a reboot or `gpupdate /force` before it's fully enforced.
- Tenable (or any compliance scanner) should pick this up after policy refresh.
- You'll still need to *actually configure a PIN* on the device with `manage-bde -protectors -add` if one isn't already set. The STIG requirement is about enforcing policy, not assigning a PIN automatically.
- **Remediation applied via PowerShell modifies the effective local security policy. Group Policy Editor will still display 'Not Configured' because this change was not**

made through a GPO template, but compliance is verified through system queries and Tenable scan results.

Status: Passed

Evidence:





---

7. Conclusion

The finding **WN11-00-000032** was successfully:

- Detected in an initial Tenable STIG Audit scan,
- Remediated manually,

- Verified through a second scan,
- Undone and confirmed as vulnerable again,
- Finally remediated Manually, and validated with a final scan.
- Testing of a PowerShell script utilizing PowerShell ISE shows remediation through Tenable. Tenable will see compliance even though `gpedit.msc` shows “Not Configured.”

This demonstrates the ability to manage Windows STIG compliance manually, and automated through PowerShell script.