

# 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"

---

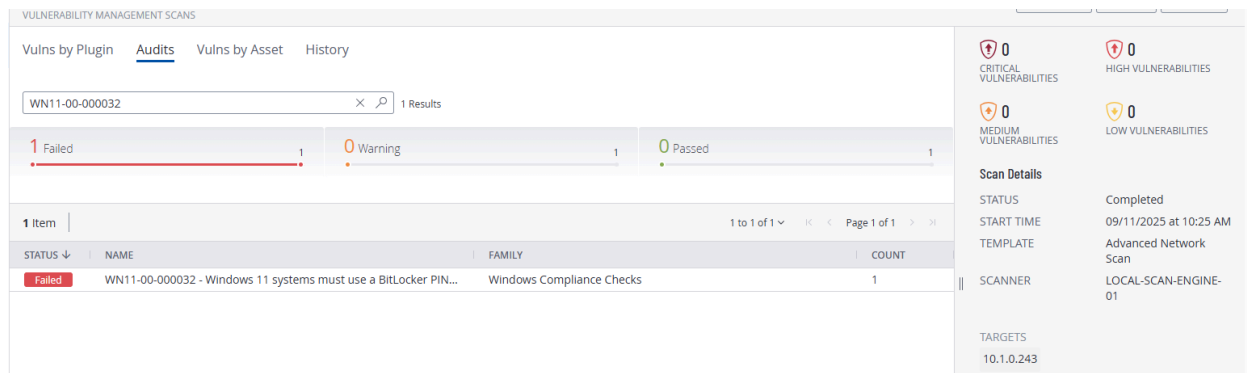
## 2. Initial Scan Results

- 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".

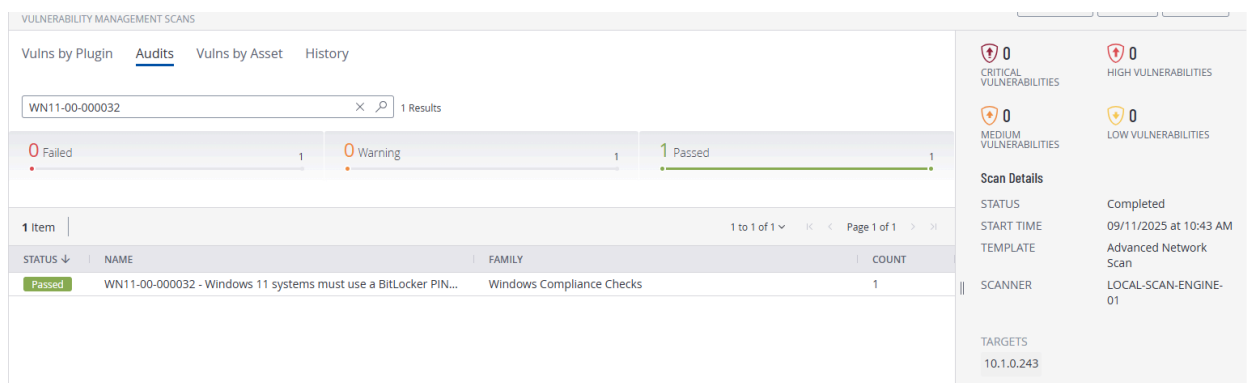
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> BitLocker Drive Encryption >> Operating System Drives "Configure minimum PIN length for startup" to "Enabled" with "Minimum characters:" set to "6" or greater.

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:

The screenshot displays the 'VULNERABILITY MANAGEMENT SCANS' interface. The 'Audits' tab is selected, showing a search for 'WN11-00-000032' with 1 result. A progress bar indicates 1 Failed, 0 Warning, and 0 Passed. The results table shows one failed item: 'WN11-00-000032 - Windows 11 systems must use a BitLocker PIN...' under the 'Windows Compliance Checks' family. The right sidebar shows zero vulnerabilities across all severity levels and scan details including status (Completed), start time (09/11/2025 at 10:55 AM), template (Advanced Network Scan), scanner (LOCAL-SCAN-ENGINE-01), and target (10.1.0.243).

STATUS	NAME	FAMILY	COUNT
Failed	WN11-00-000032 - Windows 11 systems must use a BitLocker PIN...	Windows Compliance Checks	1

---

## 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.

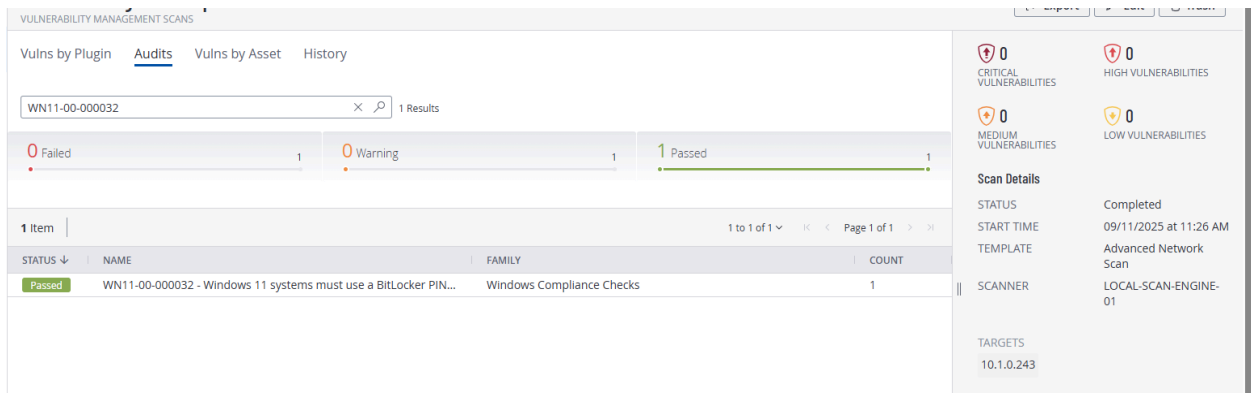
Run "gpupdate /force" and restart.

Scan again,

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

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

Evidence:

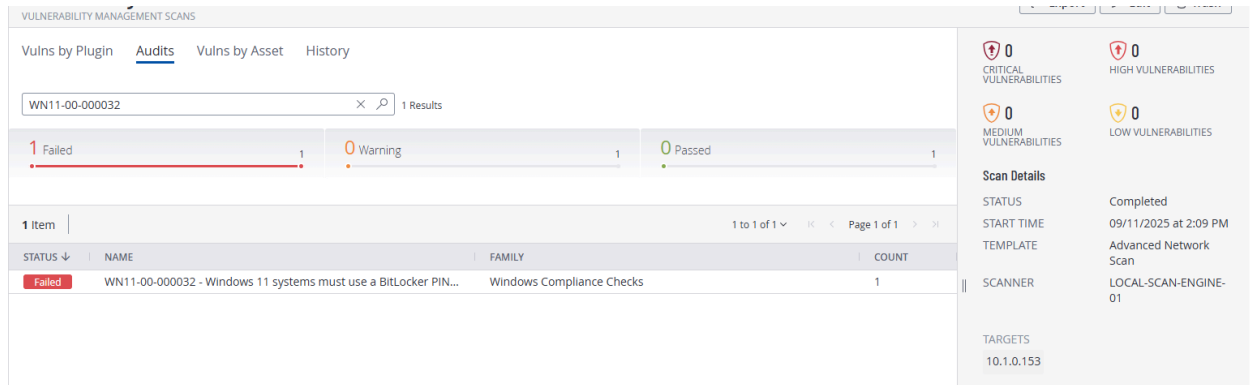


## 6. Test Remediation with PowerShell Script

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."
```

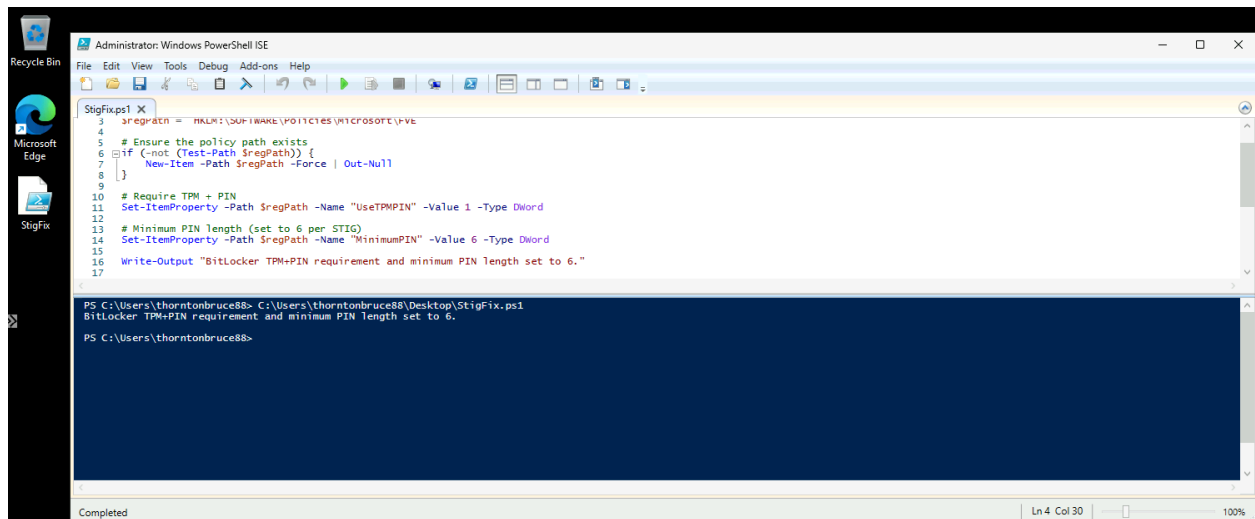
Notes:

- 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:



```
Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
StigFix.ps1 X
1 $regPath = HKLM:\SOFTWARE\POLICIES\SYSTEM\SYSTEM
2
3 # Ensure the policy path exists
4 if (-not (Test-Path $regPath)) {
5     New-Item -Path $regPath -Force | Out-Null
6 }
7
8 # Require TPM + PIN
9 Set-ItemProperty -Path $regPath -Name "UseTPMPIN" -Value 1 -Type Dword
10
11 # Minimum PIN length (set to 6 per STIG)
12 Set-ItemProperty -Path $regPath -Name "MinimumPIN" -Value 6 -Type Dword
13
14 Write-Output "BitLocker TPM+PIN requirement and minimum PIN length set to 6."
15
16
17
PS C:\Users\thorntonbruce88> C:\Users\thorntonbruce88\Desktop\StigFix.ps1
BitLocker TPM+PIN requirement and minimum PIN length set to 6.
PS C:\Users\thorntonbruce88>
```

VULNERABILITY MANAGEMENT SCANS			
Vulns by Plugin Audits Vulns by Asset History			
WN11-00-000032 1 Results			
0 Failed	1	0 Warning	1
1 Passed	1		
1 Item 1 to 1 of 1 Page 1 of 1			
STATUS	NAME	FAMILY	COUNT
Passed	WN11-00-000032 - Windows 11 systems must use a BitLocker PIN...	Windows Compliance Checks	1

0 CRITICAL VULNERABILITIES

0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES

0 LOW VULNERABILITIES

Scan Details

STATUS Completed

START TIME 09/11/2025 at 3:46 PM

TEMPLATE Advanced Network Scan

SCANNER LOCAL-SCAN-ENGINE-01

TARGETS 10.1.0.153

## 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.