STIG Implementation Report

Intern Credit Application For: Bruce Thornton
Date: 09/02/2025
STIG Finding: STIG ID: WN11-SO-000075
SRG: SRG-OS-000024-GPOS-00007
Severity: medium
CCI: CCI-000044,CCI-000048,CCI-000050 **Vulnerability ID:** V-253445

---

1. Introduction

This report documents the process of identifying, remediating, verifying, and automating the fix for a Windows 11 STIG compliance finding. The selected finding was: **STIG ID:** WN11-SO-000075 which requires that “The required legal notice must be configured to display before console logon.”

---

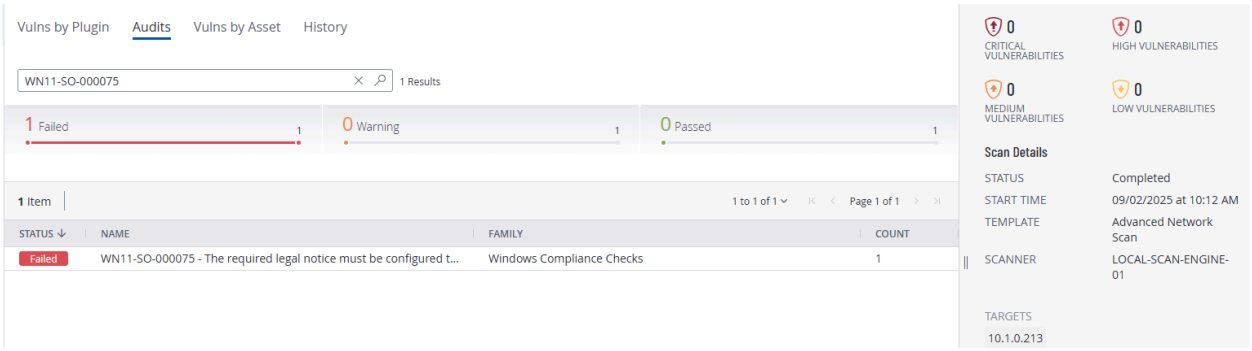
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-SO-000075
- Status: **Fail** (non-compliant)

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

https://stigaview.com/products/win11/v1r6/WN11-SO-000075/

Along with scan results:



---

3. Manual Remediation Steps

For **WN11-SO-000075**, you're working with a **Local Security Policy setting**. Here's how to do it manually step by step:

1. Press **`Win + R`**, type `gpedit.msc`, and hit **Enter**.

2. Navigate to:

Computer Configuration

└ Windows Settings

└ Security Settings

└ Local Policies

└ Security Options

3. On the right-hand side, look for:
Interactive logon: Message text for users attempting to log on

4. Double-click it, select **Enabled**, and then enter your required legal notice text in the text box.

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

5. Click **OK** and close out. Run gpupdate /force and then restart.

Important Note

There's usually a *pair* of these settings required by STIGs —

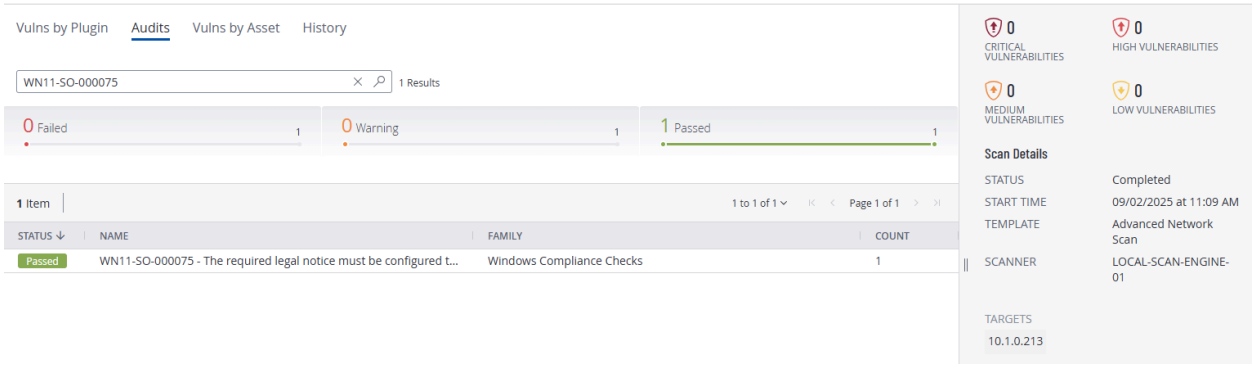
- **Message text** (this one)
- **Message title** (WN11-SO-000070)

They often go hand-in-hand because one is the heading and the other is the body of the warning notice.

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

Status: Passed

Evidence:



---

5. Reintroduction of Finding (Manually Undo Test)

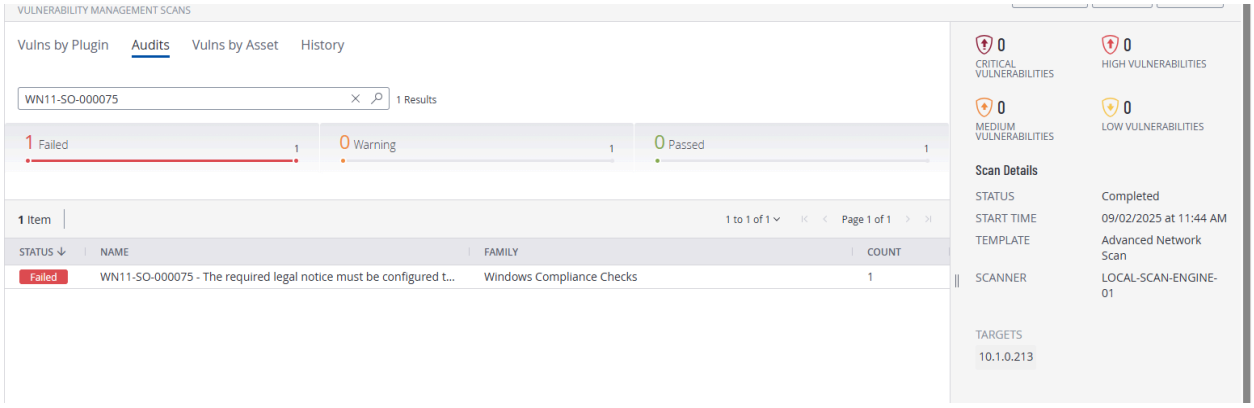
To demonstrate full control of the setting, the fix was undone:

- Disabled the setting. Ran `gpedit.msc` and followed the instructions for remediation from before and removed the text, clicked “ok.”
- Ran `gpupdate /force` and rescanned.

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

Status: Failed, Non-Compliant

Evidence:



---

6. Remediation

PowerShell Remediation

Here's how you can remediate **WN11-SO-000075** with PowerShell.

This setting is actually stored in the registry at:

- **Message Text** →
  `HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`
  Value: `LegalNoticeText` (REG_SZ)

- **Message Title** → *(usually paired, WN11-SO-000070)*
  Same key, value: `LegalNoticeCaption` (REG_SZ)

Utilized with PowerShell ISE:

Define the title (caption) and the message text

$caption = "U.S. Government Information System"

$message = @"

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

"@

Set registry keys

Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name LegalNoticeCaption -Value $caption

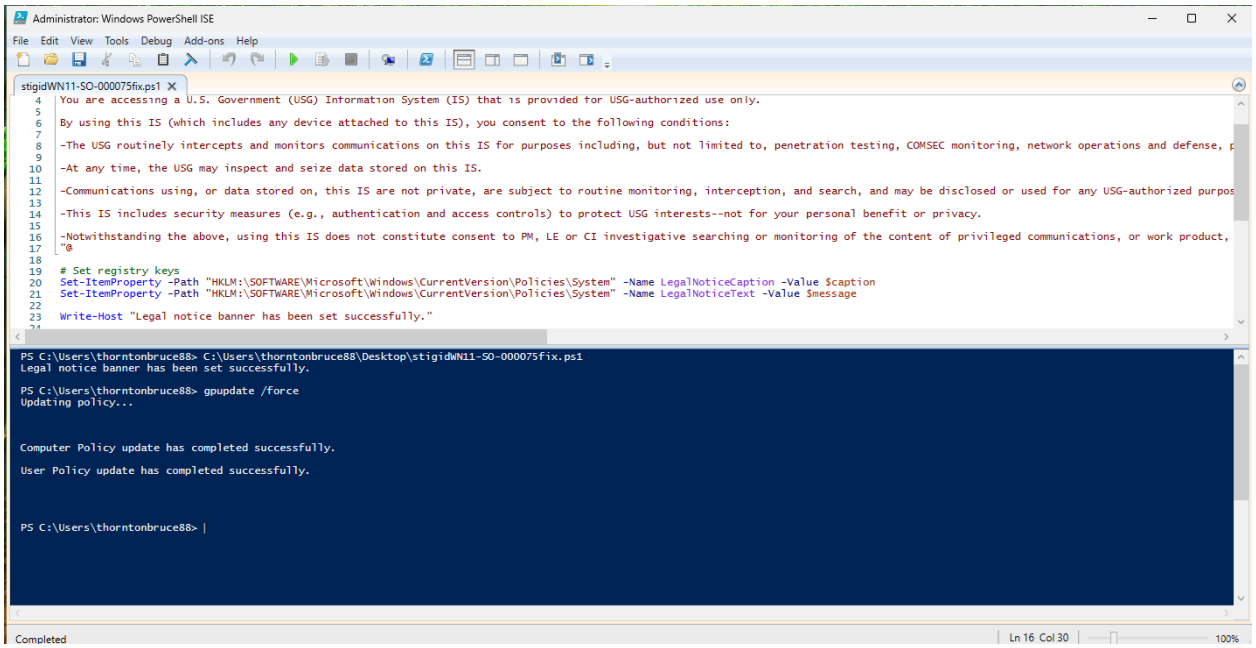
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name LegalNoticeText -Value $message

Write-Host "Legal notice banner has been set successfully."

After running this script and scanning again, Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy).

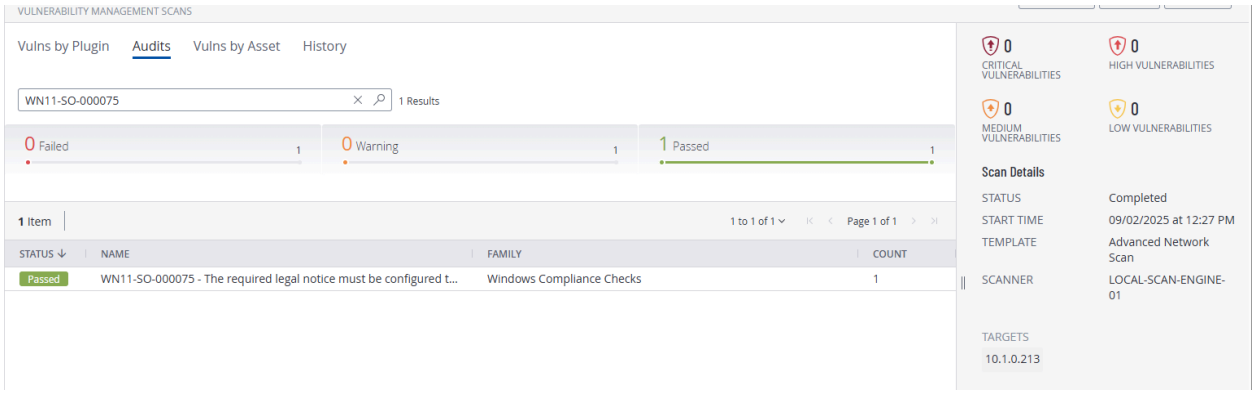
Status: Passed

Evidence:



Ran gpupdate /force, and restarted.

The required legal notice was the first output to the screen upon logging into this VM through Remote Desktop after restart.



---

7. Conclusion

The finding **WN11-SO-000075** 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.