# STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
  **Date:** 09/29/2025
  **STIG Finding:** WN11-00-000125
- **SRG:** SRG-OS-000096-GPOS-00050
  **Severity:** medium
  **Vulnerability ID:** V-268317 **CCI:** CCI-000382

---

## 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: WN11-00-000125 “Copilot in Windows must be disabled for Windows 11.”

---

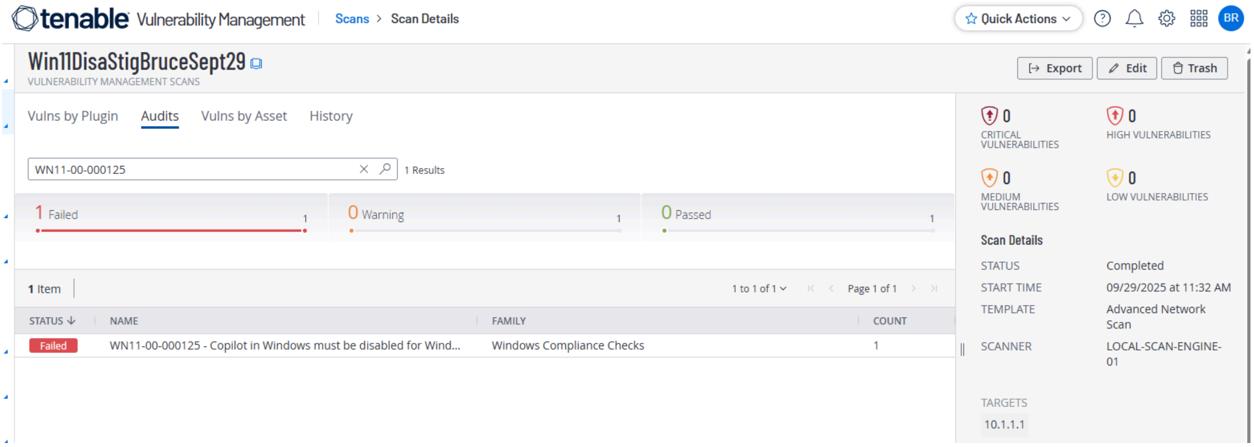
## 2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-00-000125
- Status: **Fail** (non-compliant)

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

https://stigaview.com/products/win11/v2r2/WN11-00-000125/

Initial scan result:



Win11DisaStigBruceSept29

VULNERABILITY MANAGEMENT SCANS

WN11-00-000125 — 1 Results

1 Failed 1 — 0 Warning 1 — 0 Passed 1

1 Item — 1 to 1 of 1 — Page 1 of 1

| STATUS | NAME | FAMILY | COUNT |
|---|---|---|---|
| Failed | WN11-00-000125 - Copilot in Windows must be disabled for Wind... | Windows Compliance Checks | 1 |

0 CRITICAL VULNERABILITIES — 0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES — 0 LOW VULNERABILITIES

Scan Details

| | |
|---|---|
| STATUS | Completed |
| START TIME | 09/29/2025 at 11:32 AM |
| TEMPLATE | Advanced Network Scan |
| SCANNER | LOCAL-SCAN-ENGINE-01 |

TARGETS

10.1.1.1

## 3. Manual Remediation Steps

Run “gpedit.msc”

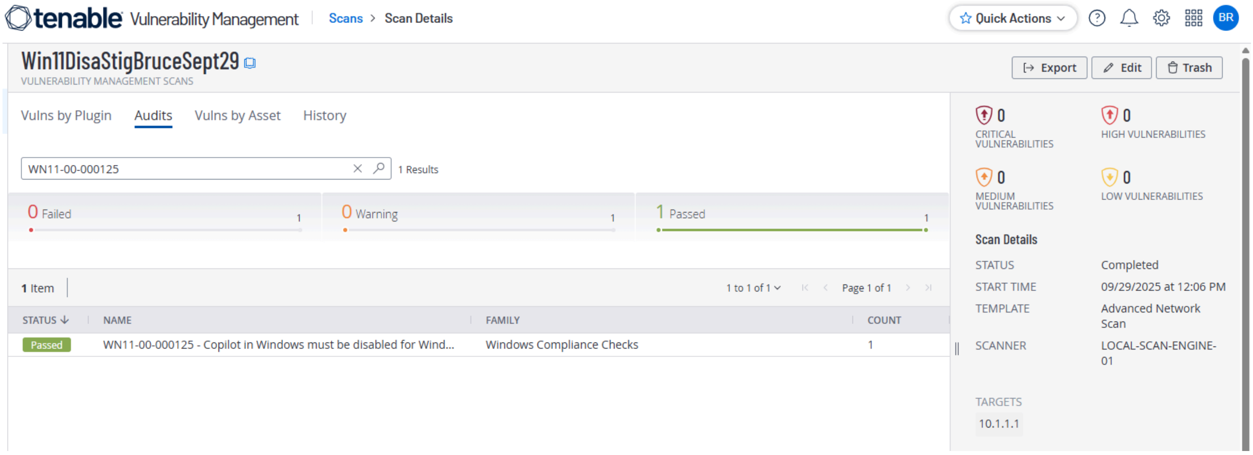
Configure the policy value for User Configuration >> Administrative Templates >> Windows Components >> Windows Copilot >> "Turn off Windows Copilot" to "Enabled"

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-00-000125
- Status: Passed

Evidence:



tenable Vulnerability Management | Scans > Scan Details

Win11DisaStigBruceSept29

VULNERABILITY MANAGEMENT SCANS

WN11-00-000125 — 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 | WN11-00-000125 - Copilot in Windows must be disabled for Wind... | Windows Compliance Checks | 1 |

0 CRITICAL VULNERABILITIES — 0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES — 0 LOW VULNERABILITIES

Scan Details

| | |
|---|---|
| STATUS | Completed |
| START TIME | 09/29/2025 at 12:06 PM |
| TEMPLATE | Advanced Network Scan |
| SCANNER | LOCAL-SCAN-ENGINE-01 |

TARGETS

10.1.1.1

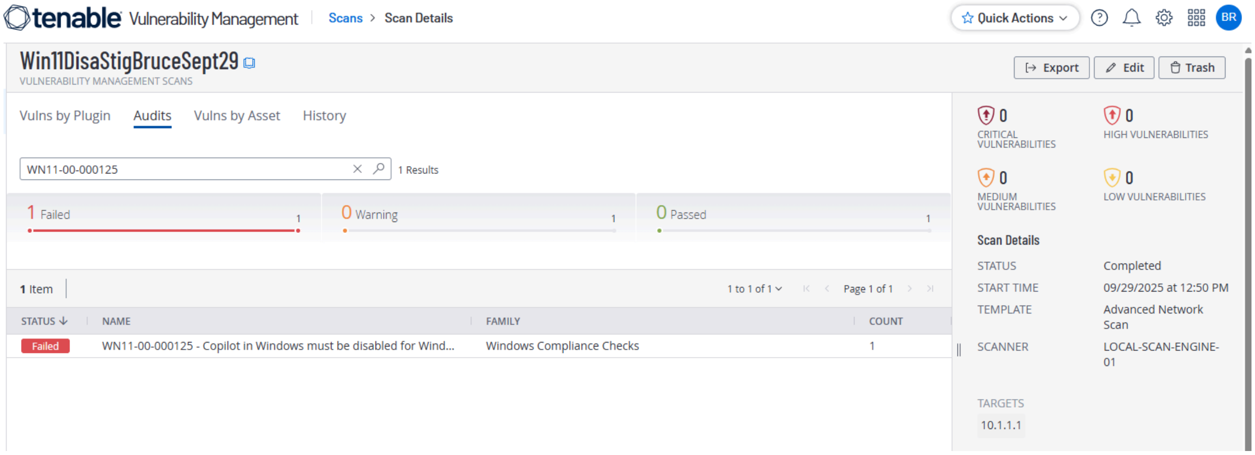
## 4. Reintroduction of Finding (Manually Undo Test)

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:



tenable Vulnerability Management | Scans > Scan Details

Win11DisaStigBruceSept29

VULNERABILITY MANAGEMENT SCANS

WN11-00-000125 — 1 Results

1 Failed 1 | 0 Warning 1 | 0 Passed 1

1 Item — 1 to 1 of 1 — Page 1 of 1

| STATUS | NAME | FAMILY | COUNT |
|---|---|---|---|
| Failed | WN11-00-000125 - Copilot in Windows must be disabled for Wind... | Windows Compliance Checks | 1 |

0 CRITICAL VULNERABILITIES — 0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES — 0 LOW VULNERABILITIES

Scan Details

| | |
|---|---|
| STATUS | Completed |
| START TIME | 09/29/2025 at 12:50 PM |
| TEMPLATE | Advanced Network Scan |
| SCANNER | LOCAL-SCAN-ENGINE-01 |

TARGETS

10.1.1.1

## 5. Remediation with PowerShell Script

**This STIG cannot be reliably remediated with a standalone PowerShell script.** It requires GPO/ADMX enforcement, because Tenable is checking the policy engine, not just registry keys.

## 5a. Manual Remediation

Run “gpedit.msc”

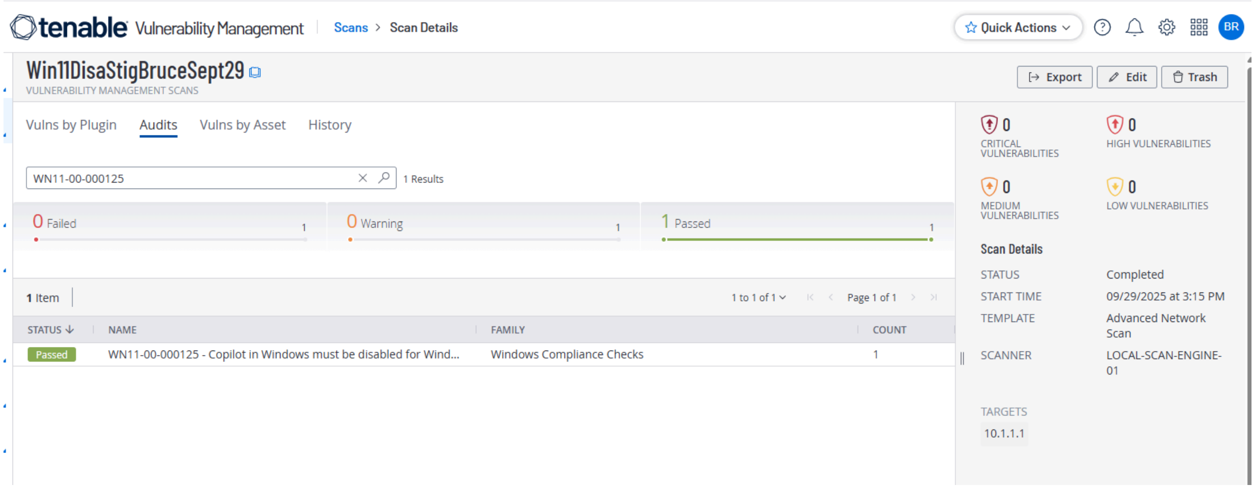
Configure the policy value for User Configuration >> Administrative Templates >> Windows Components >> Windows Copilot >> "Turn off Windows Copilot" to "Enabled"

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-00-000125
- Status: Passed

Evidence:



Win11DisaStigBruceSept29

VULNERABILITY MANAGEMENT SCANS

WN11-00-000125 — 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 | WN11-00-000125 - Copilot in Windows must be disabled for Wind... | Windows Compliance Checks | 1 |

0 CRITICAL VULNERABILITIES | 0 HIGH VULNERABILITIES

0 MEDIUM VULNERABILITIES | 0 LOW VULNERABILITIES

Scan Details

| | |
|---|---|
| STATUS | Completed |
| START TIME | 09/29/2025 at 3:15 PM |
| TEMPLATE | Advanced Network Scan |
| SCANNER | LOCAL-SCAN-ENGINE-01 |

TARGETS

10.1.1.1

## 6. Conclusion

The finding **WN11-00-000125** 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 Manual Remediation, and validated with a third scan.

This demonstrates the ability to manage Windows STIG compliance Manually for this specific Stig ID: WN11-00-000125