STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
  Date: 09/29/2025
  STIG Finding: WN11-CC-000204
- **SRG:** SRG-OS-000480-GPOS-00227
  Severity: medium
  Vulnerability ID: V-253392 **CCI:** CCI-000366

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-000204 “Enhanced diagnostic data must be limited to the minimum required to support Windows Analytics.”

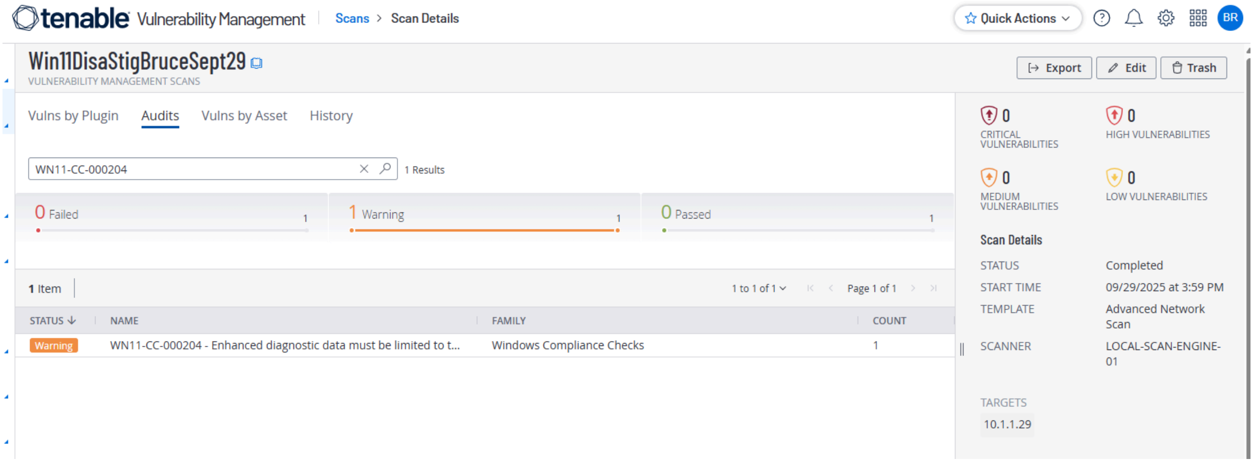
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000204
- Status: **Warning** (non-compliant)

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

https://stigaview.com/products/win11/v2r2/WN11-CC-000204/

Initial scan result:



Win11DisaStigBruceSept29
VULNERABILITY MANAGEMENT SCANS

WN11-CC-000204 — 1 Results

0 Failed 1 | 1 Warning 1 | 0 Passed 1

1 Item — 1 to 1 of 1 — Page 1 of 1

STATUS	NAME	FAMILY	COUNT
Warning	WN11-CC-000204 - Enhanced diagnostic data must be limited to t...	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 3:59 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.1.29

* The scan has returned a more urgent Status, however this status will be remediated to “Passed”

---

3. Manual Remediation Steps

Run “gpedit.msc”

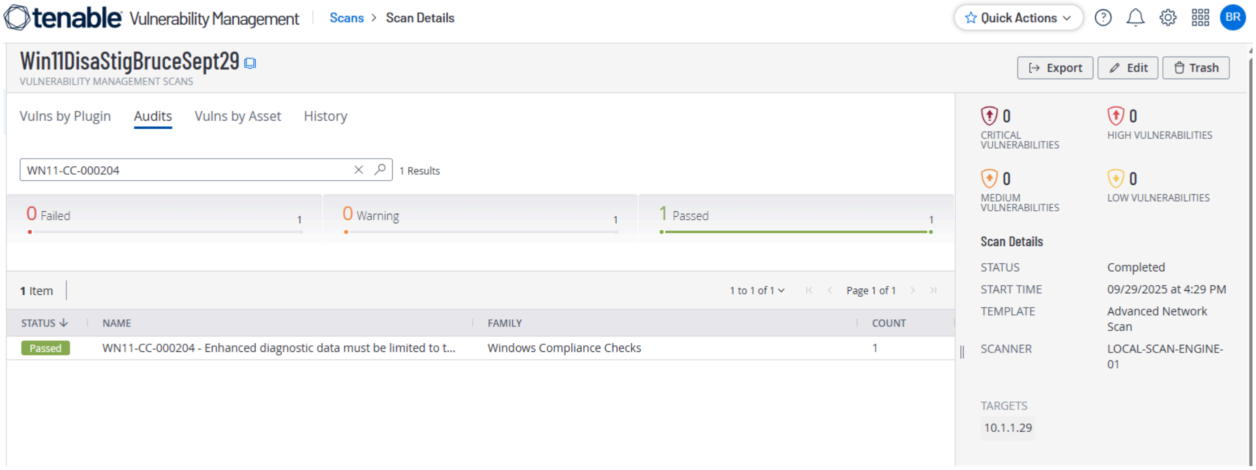
Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Data Collection and Preview Builds >> "Limit optional diagnostic data for Windows Analytics" to "Enabled" with "Enable Desktop Analytics collection" selected in "Options:"

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000204
- Status: Passed

Evidence:



Win11DisaStigBruceSept29

VULNERABILITY MANAGEMENT SCANS

WN11-CC-000204 — 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-CC-000204 - Enhanced diagnostic data must be limited to t...	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 4:29 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS

10.1.1.29

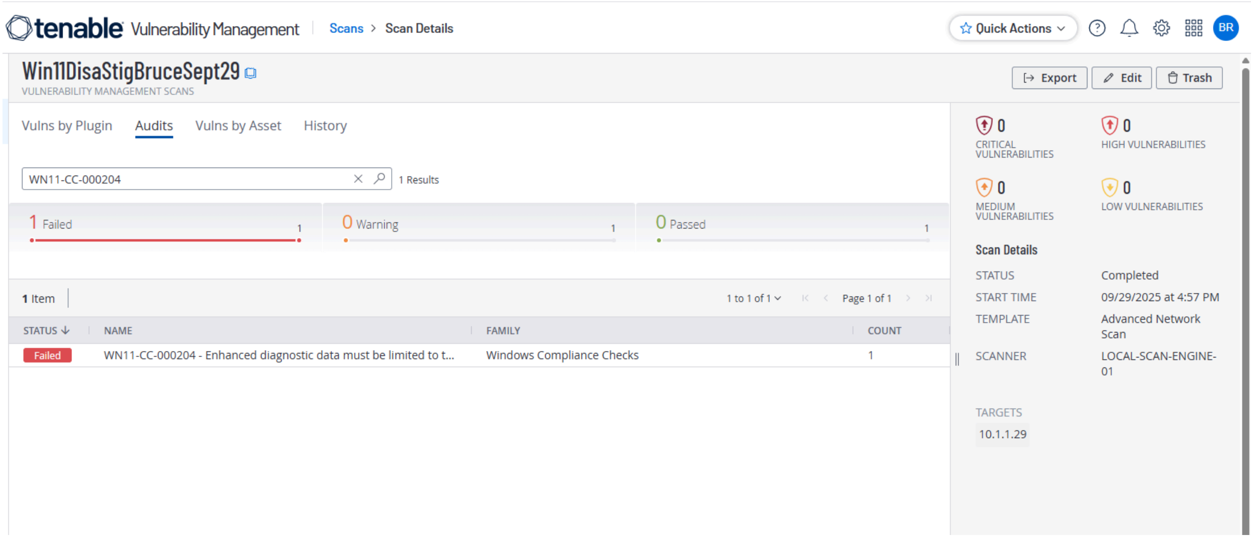
4. Reintroduction of Finding (Manually Undo Test)

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:



Win11DisaStigBruceSept29

VULNERABILITY MANAGEMENT SCANS

WN11-CC-000204 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-CC-000204 - Enhanced diagnostic data must be limited to t...	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 4:57 PM

TEMPLATE: Advanced Network Scan

SCANNER: LOCAL-SCAN-ENGINE-01

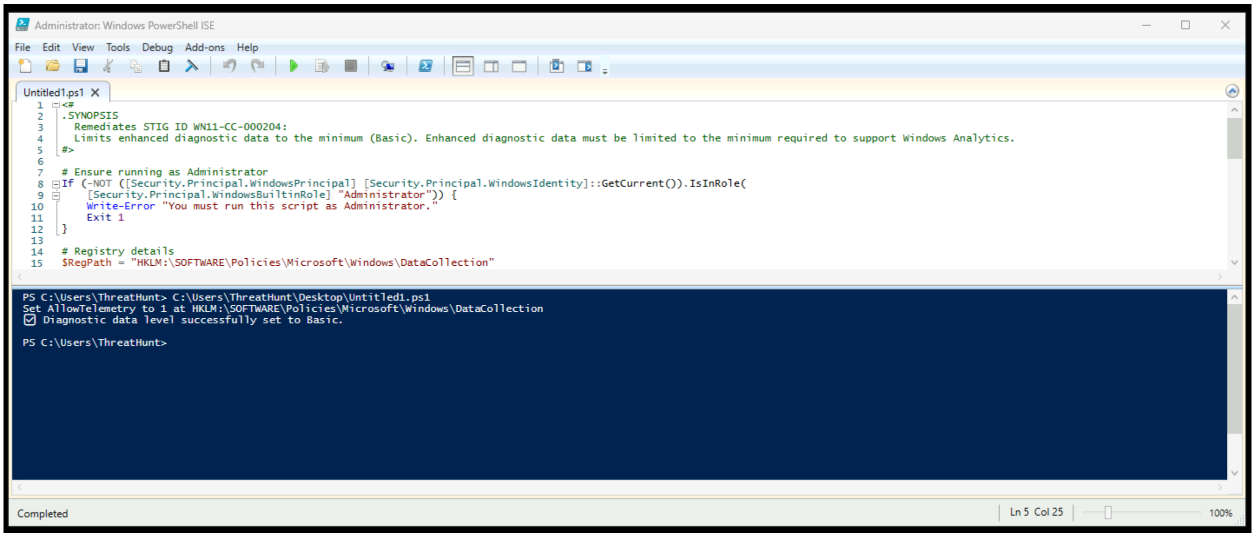
TARGETS: 10.1.1.29

5. Remediation with PowerShell Script

Utilizing PowerShell ISE, this script was ran:

```
<#
.SYNOPSIS
  Remediates STIG ID WN11-CC-000204:
  Limits enhanced diagnostic data to the minimum (Basic). Enhanced diagnostic data must be
limited to the minimum required to support Windows Analytics.
#>

# Ensure running as Administrator
If (-NOT ([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole(
    [Security.Principal.WindowsBuiltinRole] "Administrator")) {
    Write-Error "You must run this script as Administrator."
    Exit 1
}

# Registry details
$RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DataCollection"
$RegName = "AllowTelemetry"
```

```
$RegValue = 1  # Basic

# Create path if missing
If (-Not (Test-Path $RegPath)) {
    New-Item -Path $RegPath -Force | Out-Null
    Write-Output "Created registry path: $RegPath"
}

# Apply setting
Set-ItemProperty -Path $RegPath -Name $RegName -Value $RegValue -Type DWord
Write-Output "Set $RegName to $RegValue at $RegPath"

# Verify
$CurrentValue = (Get-ItemProperty -Path $RegPath -Name $RegName).$RegName
If ($CurrentValue -eq $RegValue) {
    Write-Output "✅ Diagnostic data level successfully set to Basic."
} Else {
    Write-Error "❌ Failed to apply setting. Current value: $CurrentValue"
}
```


Administrator: Windows PowerShell ISE
File Edit View Tools Debug Add-ons Help
Untitled1.ps1
Completed
Ln 5 Col 25
100%

```
<#
.SYNOPSIS
  Remediates STIG ID WN11-CC-000204:
  Limits enhanced diagnostic data to the minimum (Basic). Enhanced diagnostic data must be limited to the minimum required to support Windows Analytics.
#>

# Ensure running as Administrator
If (-NOT ([Security.Principal.WindowsPrincipal] [Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole(
    [Security.Principal.WindowsBuiltinRole] "Administrator")) {
    Write-Error "You must run this script as Administrator."
    Exit 1
}

# Registry details
$RegPath = "HKLM:\SOFTWARE\Policies\Microsoft\Windows\DataCollection"
```

```
PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Desktop\Untitled1.ps1
Set AllowTelemetry to 1 at HKLM:\SOFTWARE\Policies\Microsoft\Windows\DataCollection
☑ Diagnostic data level successfully set to Basic.

PS C:\Users\ThreatHunt>
```

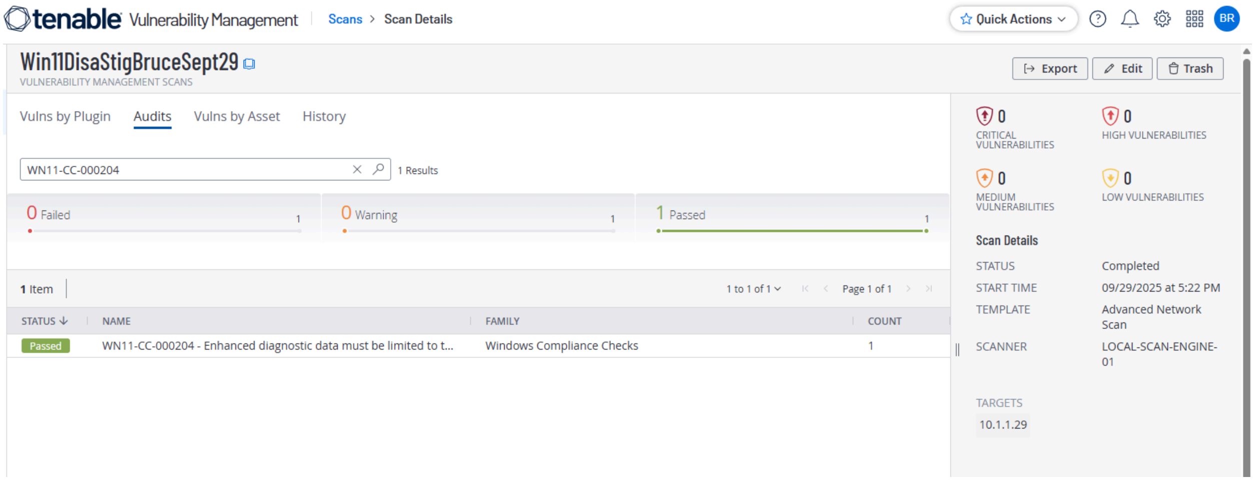
Run “gpupdate /force” and restart.

Scan again,

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

- Finding ID: WN11-CC-000204
- Status: Passed

Evidence:



Win11DisaStigBruceSept29
VULNERABILITY MANAGEMENT SCANS

WN11-CC-000204 — 1 Results

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000204 - Enhanced diagnostic data must be limited to t...	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 5:22 PM
TEMPLATE	Advanced Network Scan
SCANNER	LOCAL-SCAN-ENGINE-01

TARGETS
10.1.1.29

Notes

- Must run as **Administrator**.
- A **restart or `gpupdate /force`** may be required for Tenable to register the change.
- On **Windows 11 Home**, this policy may not exist or behave differently (but STIGs apply to Enterprise/Education builds).

---

6. Conclusion

The finding **WN11-CC-000204** 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 PowerShell automation.