STIG Implementation Report

- **Intern Credit Application For:** Bruce Thornton
  Date: 11/11/2025
  STIG Finding: WN11-CC-000391
- **SRG:** SRG-OS-000185-GPOS-00079
  Severity: medium
  Vulnerability ID: V-256893 **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-000391 “Internet Explorer must be disabled for Windows 11.”

---

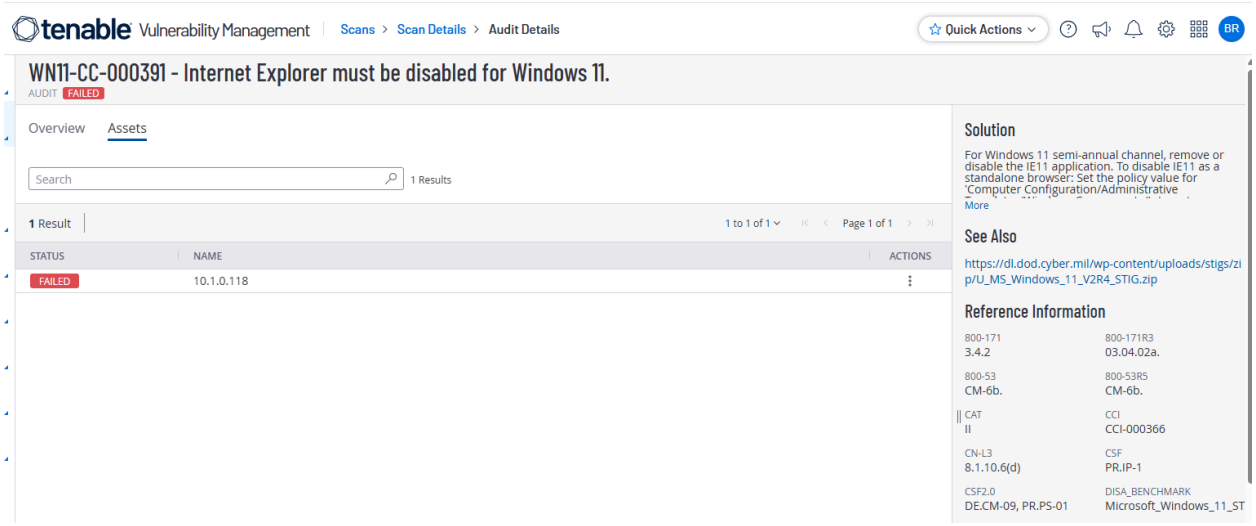
2. Initial Scan Results

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000391
- Status: **Failed** (non-compliant)

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

https://stigaview.com/products/win11/v1r5/WN11-CC-000391/

Initial scan result:



---

3. Manual Remediation Steps

For Windows 11 semi-annual channel, remove or disable the IE11 application.

To disable IE11 as a standalone browser:

Run “gpedit.msc”

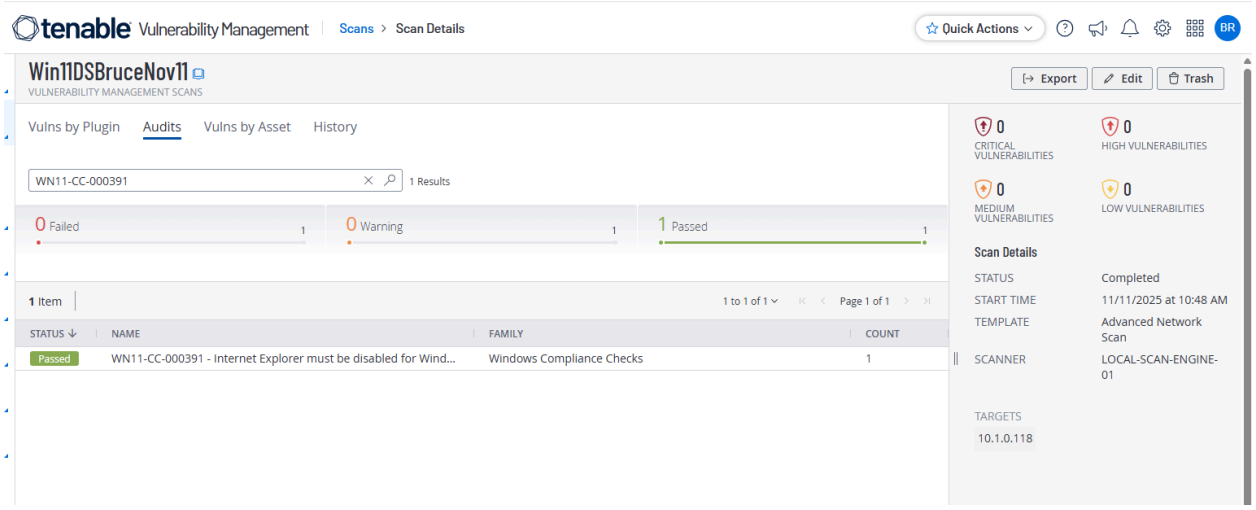
Set the policy value for "Computer Configuration/Administrative Templates/Windows Components/Internet Explorer/Disable Internet Explorer 11 as a standalone browser" to "Enabled" with the option value set to "Never".

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000391
- Status: **Passed**

Evidence:



---

4. Reintroduction of Finding (Manually Undo Test)

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

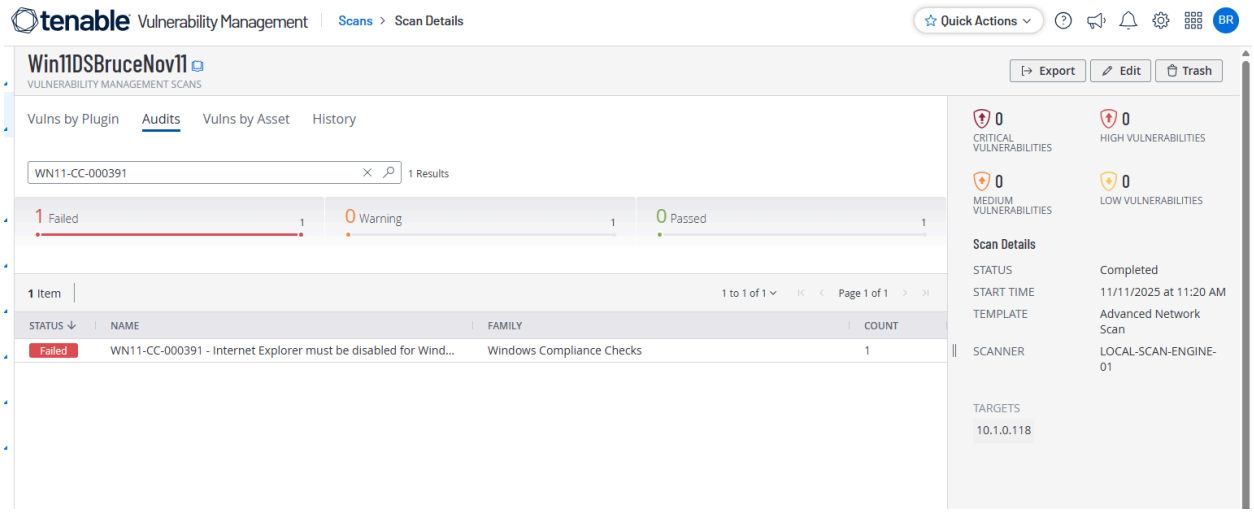
- Disabled the setting. Open Group Policy Management “gpedit.msc” and followed the instructions for remediation from before and set it to the original setting: “Not Configured”

- Ran “`gpupdate /force`” and rescanned.
- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)

- Finding ID: WN11-CC-000391

Status: **Failed**, Non-Compliant

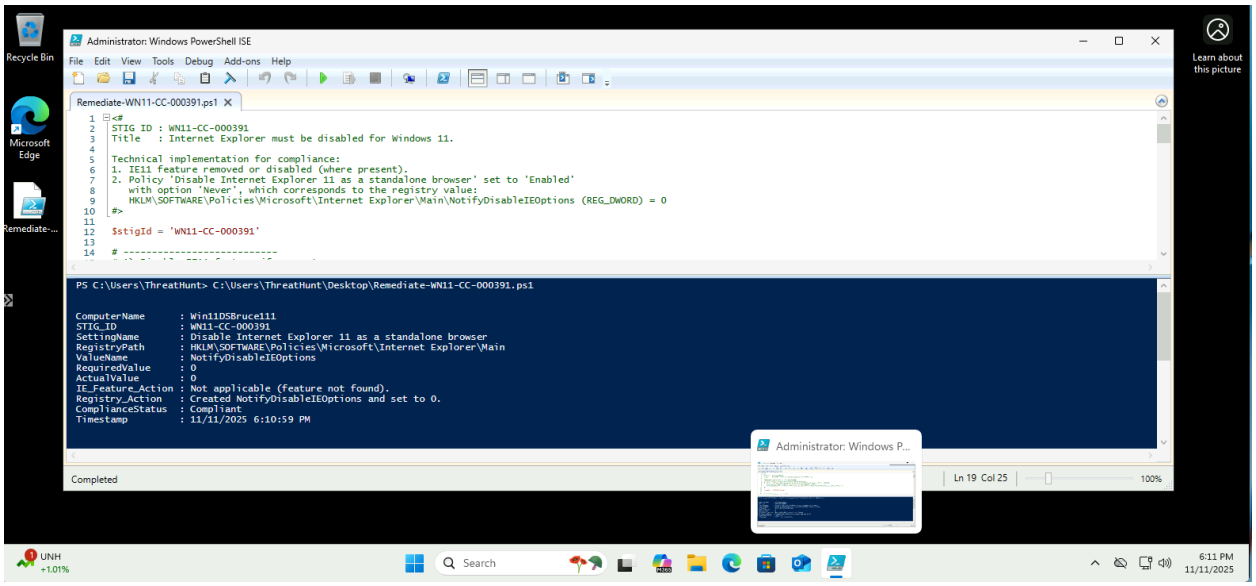
Evidence:



---

5. Remediation with PowerShell Script

Save as: `Remediate-WN11-CC-000391.ps1` and run **as Administrator** utilizing PowerShell ISE:



Script Used:

```
<#
STIG ID : WN11-CC-000391
Title   : Internet Explorer must be disabled for Windows 11.

Technical implementation for compliance:
1. IE11 feature removed or disabled (where present).
2. Policy 'Disable Internet Explorer 11 as a standalone browser' set to 'Enabled'
   with option 'Never', which corresponds to the registry value:
   HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\NotifyDisableIEOptions
(REG_DWORD) = 0
#>

$stigId = 'WN11-CC-000391'

# ----------------------------
# 1) Disable IE11 feature if present
# ----------------------------
$featureName = 'Internet-Explorer-Optional-amd64'
$feature = Get-WindowsOptionalFeature -Online -FeatureName $featureName -ErrorAction
SilentlyContinue

$featureAction = 'Not applicable (feature not found).'
if ($feature) {
    if ($feature.State -ne 'Disabled') {
        Disable-WindowsOptionalFeature -Online -FeatureName $featureName -NoRestart
-ErrorAction SilentlyContinue | Out-Null
        $featureAction = "Feature '$featureName' was enabled and has been disabled."
    } else {
        $featureAction = "Feature '$featureName' was already disabled."
    }
}

# ----------------------------
# 2) Set policy via registry
# ----------------------------
$regPath      = 'HKLM:\SOFTWARE\Policies\Microsoft\Internet Explorer\Main'
$valueName    = 'NotifyDisableIEOptions'
$desiredValue = 0   # 'Never' notify, IE11 disabled as standalone

if (-not (Test-Path $regPath)) {
    New-Item -Path $regPath -Force | Out-Null
}
```

```
$currentReg   = Get-ItemProperty -Path $regPath -Name $valueName -ErrorAction
SilentlyContinue
if ($null -eq $currentReg) {
    New-ItemProperty -Path $regPath -Name $valueName -PropertyType DWord -Value
$desiredValue -Force | Out-Null
    $regAction = "Created $valueName and set to $desiredValue."
}
elseif ($currentReg.$valueName -ne $desiredValue) {
    Set-ItemProperty -Path $regPath -Name $valueName -Value $desiredValue -Type DWord
    $regAction = "Updated $valueName from $($currentReg.$valueName) to $desiredValue."
}
else {
    $regAction = "$valueName already set to $desiredValue. No change needed."
}

# ---------------------------
# 3) Verification
# ---------------------------
$verifyReg = Get-ItemProperty -Path $regPath -Name $valueName -ErrorAction
SilentlyContinue
$actualValue = $verifyReg.$valueName

if ($actualValue -eq $desiredValue -and ($feature -eq $null -or $feature.State -eq 'Disabled')) {
    $complianceStatus = 'Compliant'
} else {
    $complianceStatus = 'Non-Compliant'
}

$result = [pscustomobject]@{
    ComputerName          = $env:COMPUTERNAME
    STIG_ID               = $stigId
    SettingName           = 'Disable Internet Explorer 11 as a standalone browser'
    RegistryPath          = 'HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Main'
    ValueName             = $valueName
    RequiredValue         = $desiredValue
    ActualValue           = $actualValue
    IE_Feature_Action     = $featureAction
    Registry_Action       = $regAction
    ComplianceStatus      = $complianceStatus
    Timestamp             = (Get-Date)
}

$result | Format-List *
# Optional CSV output for your report:
```

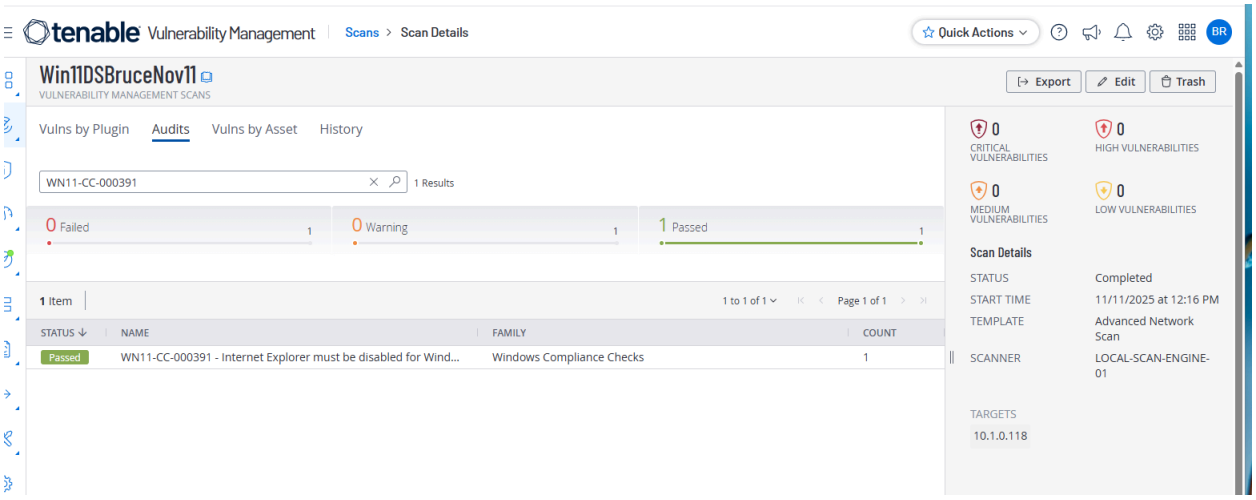
$result | Export-Csv ".\WN11-CC-000391_$($env:COMPUTERNAME).csv" -NoTypeInformation -Append

Run “gpupdate /force” and restart.

Scan again,

- Tool: Tenable.sc / Nessus (Windows 11 STIG Audit Policy)
- Finding ID: WN11-CC-000391
- Status: **Passed**

Evidence:



---

6. Conclusion

The finding **WN11-CC-000391** 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.