

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:

The screenshot displays the Tenable Vulnerability Management interface. The top navigation bar includes the Tenable logo, 'Vulnerability Management', and a breadcrumb trail: 'Scans > Scan Details > Audit Details'. On the right, there are icons for 'Quick Actions', help, notifications, settings, and a 'BR' button. The main header shows the audit title 'WN11-CC-000391 - Internet Explorer must be disabled for Windows 11.' with a red 'FAILED' status indicator. Below the header, there are tabs for 'Overview' and 'Assets'. A search bar with the text '1 Results' is present. A table lists the audit results, showing one entry with a 'FAILED' status and the name '10.1.0.118'. To the right of the table, there is a 'Solution' section with instructions for Windows 11, a 'See Also' link to a STIG zip file, and a 'Reference Information' table listing various identifiers.

STATUS	NAME	ACTIONS
FAILED	10.1.0.118	

Solution
For Windows 11 semi-annual channel, remove or disable the IE11 application. To disable IE11 as a standalone browser: Set the policy value for "Computer Configuration/Administrative Templates/Windows Components/Internet Explorer/Disable Internet Explorer 11 as a standalone browser" to "Enabled".

See Also
https://dl.dod.cyber.mil/wp-content/uploads/stigs/zip/U_MS_Windows_11_V2R4_STIG.zip

Reference Information

800-171 3.4.2	800-171R3 03.04.02a.
800-53 CM-6b.	800-53R5 CM-6b.
CAT II	CCI CCI-000366
CN-L3 8.1.10.6(d)	CSF PR.IP-1
CSF2.0 DE.CM-09, PR.PS-01	DISA_BENCHMARK Microsoft_Windows_11_ST

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"

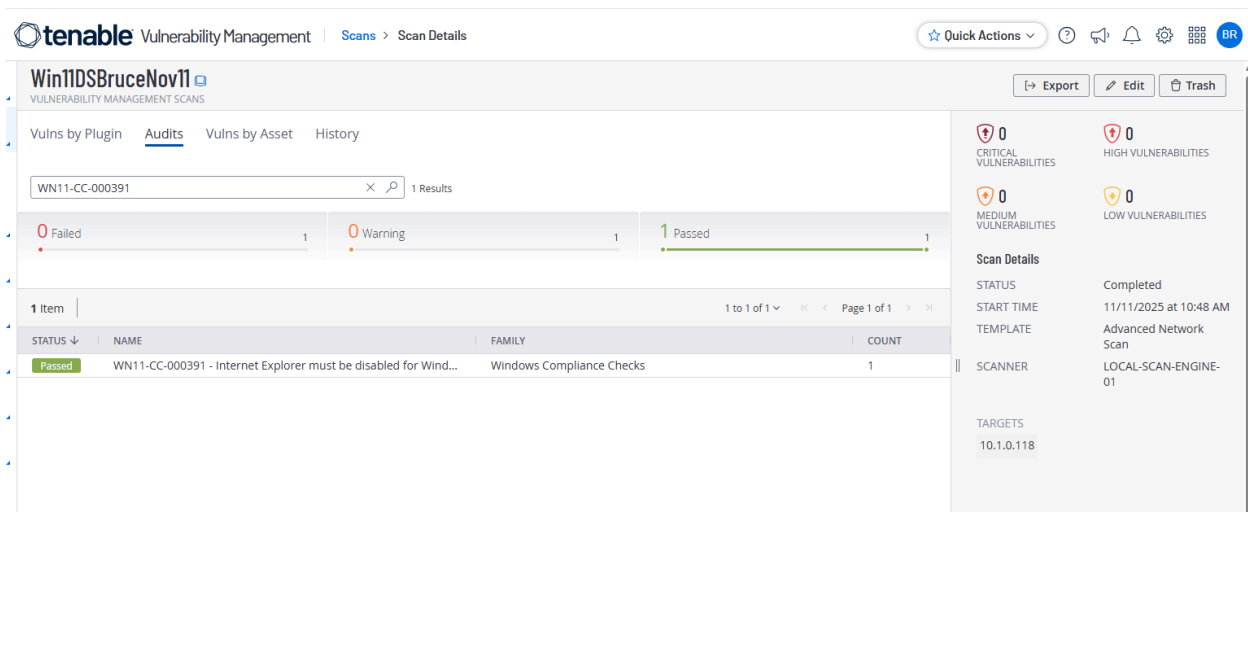
Set the policy value for "Computer Configuration/Administrative Templates/Windows Components/Internet Explorer/Disable Internet Explorer 11 as a standalone browser" to "Enabled" with the option value set to "Never".

Run "gpupdate /force" and restart.

Scan again,

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

Evidence:



tenable Vulnerability Management | Scans > Scan Details

Win11DSBruceNov11
VULNERABILITY MANAGEMENT SCANS

Export Edit Trash

Vulns by Plugin Audits Vulns by Asset History

WN11-CC-000391 1 Results

0 Failed 0 Warning 1 Passed

1 Item

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000391 - Internet Explorer must be disabled for Wind...	Windows Compliance Checks	1

1 to 1 of 1 < > Page 1 of 1 >>

Scan Details

STATUS Completed

START TIME 11/11/2025 at 10:48 AM

TEMPLATE Advanced Network Scan

SCANNER LOCAL-SCAN-ENGINE-01

TARGETS 10.1.0.118

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:

The screenshot shows the Tenable Vulnerability Management interface. The top navigation bar includes 'tenable Vulnerability Management', 'Scans', and 'Scan Details'. The main header displays 'Win11DSBruceNov11' and 'VULNERABILITY MANAGEMENT SCANS'. Below this, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. A search bar contains 'WN11-CC-000391' and shows '1 Results'. A progress bar indicates 1 Failed, 0 Warning, and 0 Passed. A table lists the scan results:

STATUS	NAME	FAMILY	COUNT
Failed	WN11-CC-000391 - Internet Explorer must be disabled for Wind...	Windows Compliance Checks	1

On the right, a 'Scan Details' panel shows:

- CRITICAL VULNERABILITIES: 0
- HIGH VULNERABILITIES: 0
- MEDIUM VULNERABILITIES: 0
- LOW VULNERABILITIES: 0
- STATUS: Completed
- START TIME: 11/11/2025 at 11:20 AM
- TEMPLATE: Advanced Network Scan
- SCANNER: LOCAL-SCAN-ENGINE-01
- TARGETS: 10.1.0.118

5. Remediation with PowerShell Script

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

The screenshot shows the PowerShell ISE interface with the script 'Remediate-WN11-CC-000391.ps1' open. The script content is as follows:

```
1 STIG ID : WN11-CC-000391
2 Title : Internet Explorer must be disabled for Windows 11.
3
4
5 Technical implementation for compliance:
6 1. IE11 feature removed or disabled (where present).
7 2. Policy 'Disable Internet Explorer 11 as a standalone browser' set to 'Enabled'
8 with option 'Never', which corresponds to the registry value:
9 HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Main\NotifyDisableIEOptions (REG_DWORD) = 0
10
11 $stigid = 'WN11-CC-000391'
12
13 # -----
14
```

The output of the script is displayed in the console window:

```
PS C:\Users\ThreatHunt> C:\Users\ThreatHunt\Desktop\Remediate-WN11-CC-000391.ps1

ComputerName : Win11DSBruce11
STIG_ID      : WN11-CC-000391
SettingName  : Disable Internet Explorer 11 as a standalone browser
RegistryPath : HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\Main
ValueName    : NotifyDisableIEOptions
RequiredValue : 0
ActualValue  : 0
IE_Feature_Action : Not applicable (feature not found).
Registry_Action : Created NotifyDisableIEOptions and set to 0.
ComplianceStatus : Compliant
Timestamp    : 11/11/2025 6:10:59 PM
```

The status bar at the bottom indicates 'Completed' and 'Ln 19 Col 25'.

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:

The screenshot displays the Tenable Vulnerability Management interface. The top navigation bar shows 'tenable Vulnerability Management' and 'Scans > Scan Details'. The main header identifies the scan as 'Win11DSBruceNov11' with the subtitle 'VULNERABILITY MANAGEMENT SCANS'. On the right, there are buttons for 'Export', 'Edit', and 'Trash'. Below the header, there are tabs for 'Vulns by Plugin', 'Audits', 'Vulns by Asset', and 'History'. The 'Audits' tab is active, showing a search bar with 'WN11-CC-000391' and '1 Results'. A progress bar indicates 0 Failed, 0 Warning, and 1 Passed. Below this, a table lists the results:

STATUS	NAME	FAMILY	COUNT
Passed	WN11-CC-000391 - Internet Explorer must be disabled for Wind...	Windows Compliance Checks	1

On the right side, a 'Scan Details' panel shows: STATUS: Completed, START TIME: 11/11/2025 at 12:16 PM, TEMPLATE: Advanced Network Scan, SCANNER: LOCAL-SCAN-ENGINE-01, and TARGETS: 10.1.0.118. At the top right of the details panel, there are four vulnerability counts: 0 CRITICAL VULNERABILITIES, 0 HIGH VULNERABILITIES, 0 MEDIUM VULNERABILITIES, and 0 LOW VULNERABILITIES.

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.