

Forum:[Hack Forums](#)

Thread: [CVE202550154 zero-click Windows File Explorer spoofing vulnerability | Patch script](#)

Curs3d - August 21, 2025, 11:13 am

CVE-2025-50154 is a zero-click Windows File Explorer spoofing vulnerability. Public research indicates it may coerce NTLM authentication or fetch remote content via crafted paths or shortcuts, potentially deceiving users and leaking credentials for follow-on compromise.

Recommended actions:

- Apply Microsoft's August 2025 security update: it fully addresses this zero-click NTLM leak and related spoofing avenues.
- Disable NTLM authentication in environments that use Kerberos, or limit NTLM usage to trusted scenarios only.

Vicarius Labs has created a mitigation script to apply temporary protection

Spoiler ([Click to View](#))Code <#

.SYNOPSIS

Applies mitigations for CVE-2025-50154.

.DESCRIPTION

This script implements mitigations by denying NTLM traffic, disabling WebClient service, and blocking outbound SMB traffic.

.EXECUTION

Run this script in PowerShell as Administrator for proper execution.

#>

TAG CONFIGURATION

\$TagInfo = "[Info]"

\$TagSuccess = "[Success]"

\$TagWarn = "[Warning]"

\$TagErr = "[Error]"

Status function

function Write-Status {

param(

[string]\$Message,

[ValidateSet("Info","Success","Warning","Error")][string]\$Level = "Info"

)

\$tag = switch (\$Level) {

"Info" { \$TagInfo }

"Success" { \$TagSuccess }

"Warning" { \$TagWarn }

"Error" { \$TagErr }

}

Write-Host "\$tag \$Message"

}

```

Write-Status "CVE-2025-50154 Mitigation Script" "Info"
Write-Status "===== " "Info"
Write-Host ""
Write-Status "DISCLAIMER: Mitigations are intended only as temporary measures and might not
fully protect your system from CVE-2025-50154. Whenever possible, install the latest security
patches to ensure complete protection." "Warning"
Write-Host ""

# Check if running as Administrator
$isAdmin = ([Security.Principal.WindowsPrincipal]
[Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]
"Administrator")
if (-not $isAdmin) {
    Write-Status "This script requires Administrator privileges for proper execution." "Warning"
}

# Mitigation 1: Deny outgoing NTLM traffic
Write-Status "Applying Mitigation 1: Denying outgoing NTLM traffic..." "Info"
try {
    $lsaPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\MSV1_0"

    # Ensure the registry path exists
    if (-not (Test-Path $lsaPath)) {
        New-Item -Path $lsaPath -Force | Out-Null
    }

    # Set RestrictSendingNTLMTraffic to 2 (Deny all)
    Set-ItemProperty -Path $lsaPath -Name "RestrictSendingNTLMTraffic" -Value 2 -Type DWord
    Write-Status "Successfully configured to deny outgoing NTLM traffic." "Success"

} catch {
    Write-Status "Failed to configure NTLM restrictions: $($_.Exception.Message)" "Error"
}

# Mitigation 2: Disable WebClient (WebDAV) service
Write-Status "Applying Mitigation 2: Disabling WebClient service..." "Info"
try {
    $webClientService = Get-Service -Name "WebClient" -ErrorAction Stop

    # Stop the service if it's running
    if ($webClientService.Status -eq "Running") {
        Stop-Service -Name "WebClient" -Force
        Write-Status "WebClient service stopped." "Success"
    }

    # Disable the service
    Set-Service -Name "WebClient" -StartupType Disabled
    Write-Status "WebClient service disabled successfully." "Success"

} catch {
    Write-Status "Failed to disable WebClient service: $($_.Exception.Message)" "Error"
}

```

Mitigation 3: Block outbound SMB traffic (TCP 445/139)

Write-Status "Applying Mitigation 3: Blocking outbound SMB traffic..." "Info"

```
try {
    # Block outbound SMB traffic on port 445
    $rule445Name = "Block Outbound SMB 445 - CVE-2025-50154 Mitigation"
    $existingRule445 = Get-NetFirewallRule -DisplayName $rule445Name -ErrorAction
    SilentlyContinue

    if (-not $existingRule445) {
        New-NetFirewallRule -DisplayName $rule445Name -Direction Outbound -Protocol TCP
    -RemotePort 445 -Action Block -Profile Any
        Write-Status "Created firewall rule to block outbound SMB traffic on port 445." "Success"
    } else {
        Write-Status "Firewall rule for blocking outbound SMB port 445 already exists." "Info"
    }

    # Block outbound SMB traffic on port 139
    $rule139Name = "Block Outbound SMB 139 - CVE-2025-50154 Mitigation"
    $existingRule139 = Get-NetFirewallRule -DisplayName $rule139Name -ErrorAction
    SilentlyContinue

    if (-not $existingRule139) {
        New-NetFirewallRule -DisplayName $rule139Name -Direction Outbound -Protocol TCP
    -RemotePort 139 -Action Block -Profile Any
        Write-Status "Created firewall rule to block outbound SMB traffic on port 139." "Success"
    } else {
        Write-Status "Firewall rule for blocking outbound SMB port 139 already exists." "Info"
    }

} catch {
    Write-Status "Failed to create SMB blocking firewall rules: $($_.Exception.Message)" "Error"
}

Write-Host ""
Write-Status "Mitigation Summary:" "Info"
Write-Status "===== " "Info"
Write-Status "1. Outgoing NTLM traffic denial configured" "Info"
Write-Status "2. WebClient (WebDAV) service disabled" "Info"
Write-Status "3. Outbound SMB traffic blocked (ports 445, 139)" "Info"
Write-Host ""
Write-Status "IMPORTANT: A system restart may be required for some changes to take full effect."
"Warning"
Write-Status "These mitigations are temporary measures. Apply official security patches when
available." "Warning"
```