How to Disable Remote Desktop Protocol Connection Using Automox

This worklet describes how to disable remote desktop services.

If a machine is unpatchable, security administrators can use this worklet as a mitigating control to protect impacted Windows systems from the BlueKeep vulnerability. This worklet also can act as a general security hardening on all Windows devices with newer operating systems not vulnerable to the specific threat.

To deploy this device hardening worklet, do the following:

1. Log in to your Automox console.
2. Browse to the System Management page and click Create Policy.
3. Click Worklet.
4. Click Next.
5. On the Create Worklet page, enter a name for the new worklet and select Windows.
6. Insert the Evaluation and Remediation Code scripts. The evaluation code keeps you apprised of each device’s ongoing compliance, as well as flags the device for remediation. The remediation code enforces this setting on the schedule you define.

Evaluation Code
# Define Registry Key and sub-value to evaluate
#############################################
$regPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server"
$regProperty = "fDenyTSConnections"
$desiredValue = '1'
#############################################

# Retrieve current value for comparison
$currentValue = (Get-ItemProperty -Path $regPath -Name $regProperty).$regProperty

# Compare current with desired and exit accordingly.
# 0 for Compliant, 1 for Non-Compliant
if ($currentValue -eq $desiredValue) {
    Exit 0
} else { Exit 1 }

# Define Registry Key and sub-value to modify
#############################################
$regPath = "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server"
$regProperty = "fDenyTSConnections"
$desiredValue = '1'
#############################################

try {
    Set-ItemProperty -Path $regPath -Name $regProperty -Value $desiredValue
    Exit 0
} catch {
    Write-Output "Unable to update $regProperty"
    Exit 1
}
7. After setting a schedule, click **Create Policy**.