

Disabling Windows Print Spooler Service on AIDA HD Connect (CVE-2021-34527)

August 17, 2021

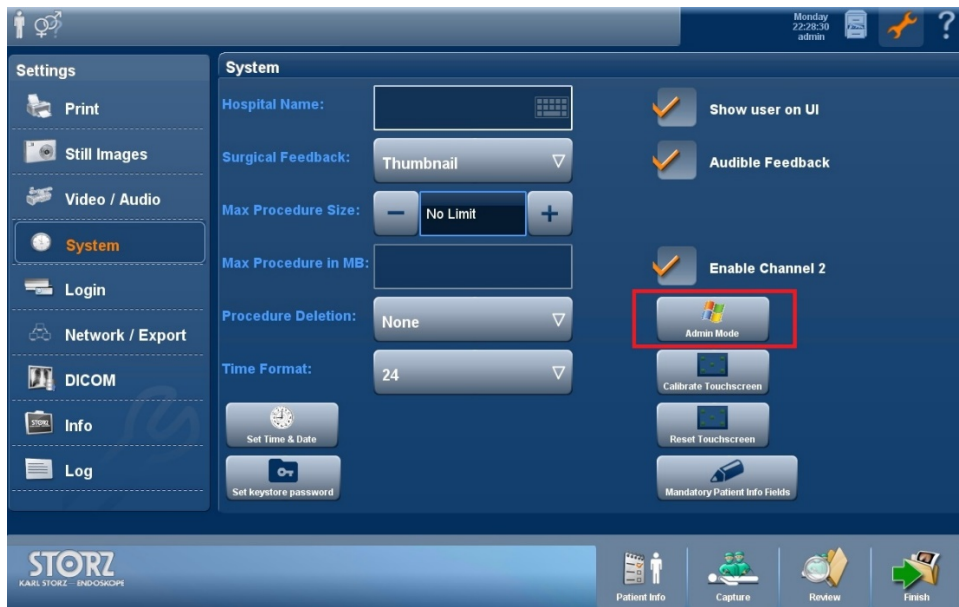
Overview:

The objective of this document is to illustrate how to disable the Windows Print Spooler service to mitigate the Microsoft Windows vulnerability CVE-2021-34527 on AIDA HD Connect (WES7 system).

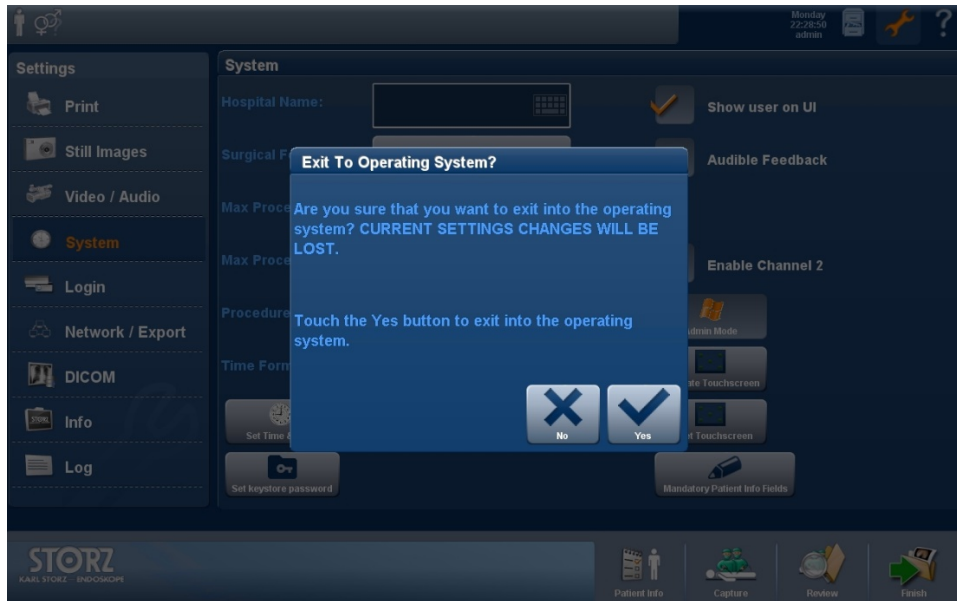
Procedures:

1. Admin mode

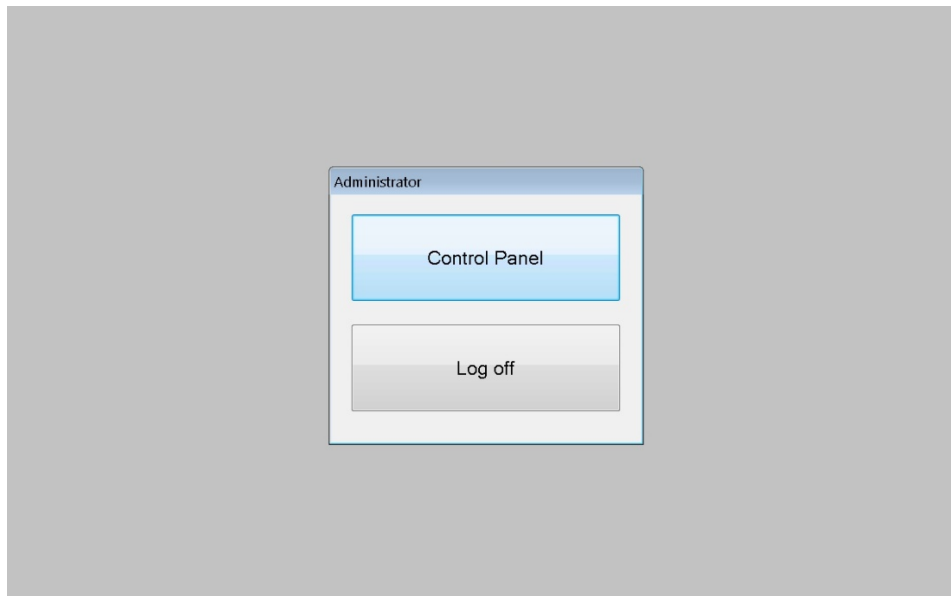
Logon System as an admin user. Select System -> Admin Mode



2. Exit to the Windows OS

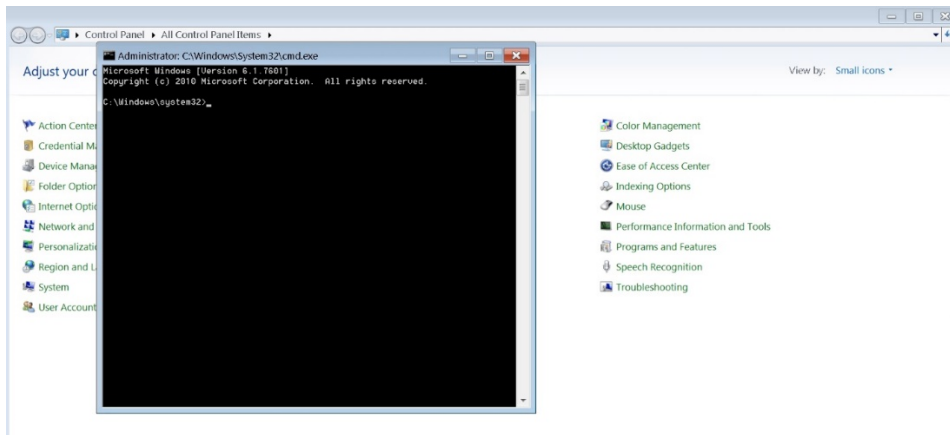
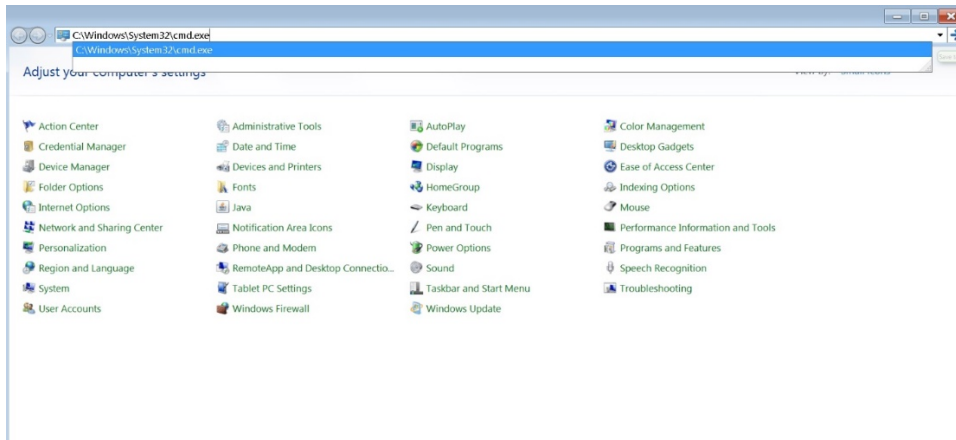


3. Select Control Panel



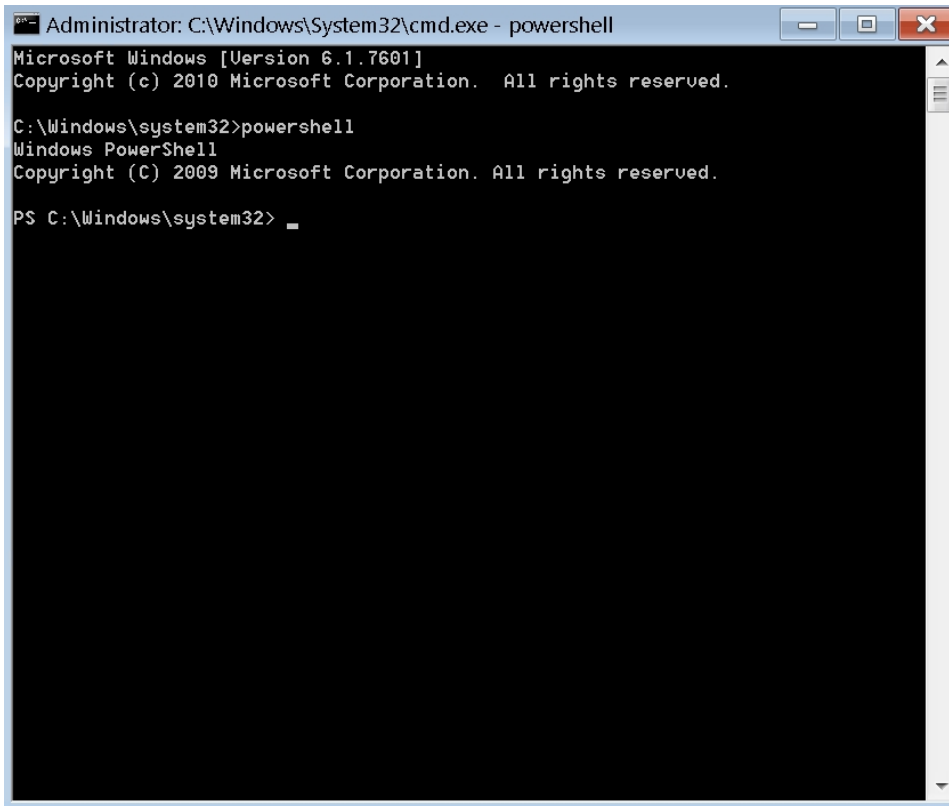
4. Open the System CMD Window

Type "C:\Windows\System32\cmd.exe" and press enter



5. Run Powershell

Type "powershell" on the command line and press enter



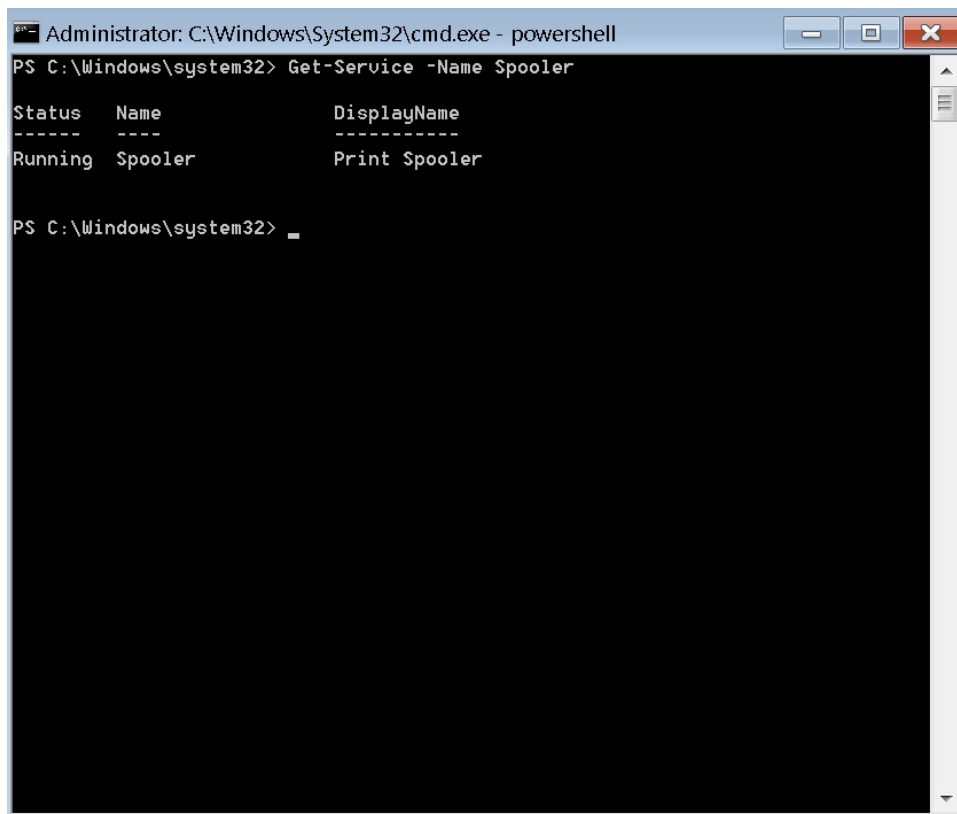
```
Administrator: C:\Windows\System32\cmd.exe - powershell
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2010 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powershell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> _
```

6. Get Print Spooler Status

Run `Get-Service -Name Spooler` to check the status



```
Administrator: C:\Windows\System32\cmd.exe - powershell
PS C:\Windows\system32> Get-Service -Name Spooler

Status      Name      DisplayName
-----
Running     Spooler   Print Spooler

PS C:\Windows\system32> _
```

7. Stop Print Spooler Service

Run `Stop-Service -Name Spooler -Force` and check the status `Get-Service -Name Spooler`. The status of Spooler should now be "Stopped".

```
Administrator: C:\Windows\System32\cmd.exe - powershell
PS C:\Windows\system32> Get-Service -Name Spooler

Status   Name          DisplayName
-----   -
Running  Spooler       Print Spooler

PS C:\Windows\system32> Stop-Service -Name Spooler -Force
PS C:\Windows\system32>
PS C:\Windows\system32> Get-Service -Name Spooler

Status   Name          DisplayName
-----   -
Stopped  Spooler       Print Spooler

PS C:\Windows\system32> _
```

8. Disable Print Spooler Service

To disable the Print Spooler service type `Set-Service -Name Spooler -StartupType Disabled` and the Spooler service will not be run on system startup.

```
Administrator: C:\Windows\System32\cmd.exe - powershell
PS C:\Windows\system32> Get-Service -Name Spooler

Status  Name          DisplayName
-----  -
Running Spooler      Print Spooler

PS C:\Windows\system32> Stop-Service -Name Spooler -Force
PS C:\Windows\system32>
PS C:\Windows\system32> Get-Service -Name Spooler

Status  Name          DisplayName
-----  -
Stopped Spooler      Print Spooler

PS C:\Windows\system32> Set-Service -Name Spooler -StartupType Disabled
PS C:\Windows\system32>
PS C:\Windows\system32> Get-Service -Name Spooler

Status  Name          DisplayName
-----  -
Stopped Spooler      Print Spooler

PS C:\Windows\system32> _
```

9. Exit powershell and CMD

```
Administrator: C:\Windows\System32\cmd.exe
PS C:\Windows\system32> Get-Service -Name Spooler

Status  Name          DisplayName
-----  -
Running Spooler      Print Spooler

PS C:\Windows\system32> Stop-Service -Name Spooler -Force
PS C:\Windows\system32>
PS C:\Windows\system32> Get-Service -Name Spooler

Status  Name          DisplayName
-----  -
Stopped Spooler      Print Spooler

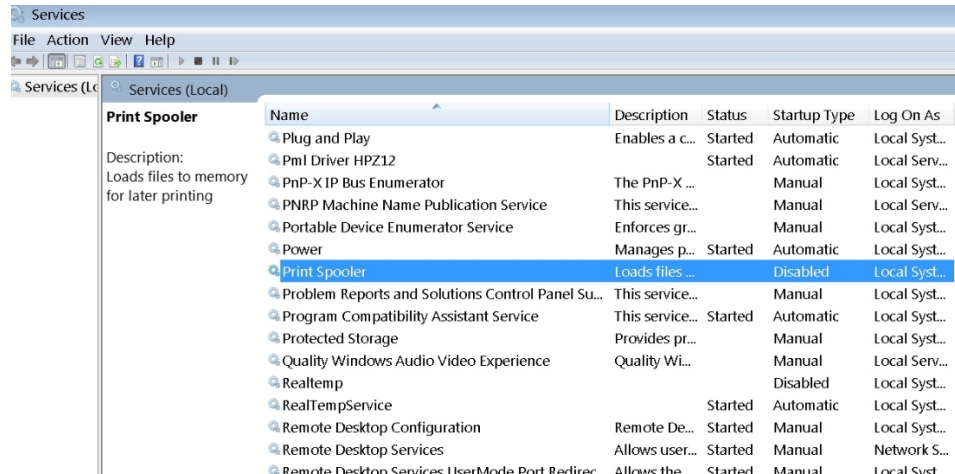
PS C:\Windows\system32> Set-Service -Name Spooler -StartupType Disabled
PS C:\Windows\system32>
PS C:\Windows\system32> Get-Service -Name Spooler

Status  Name          DisplayName
-----  -
Stopped Spooler      Print Spooler

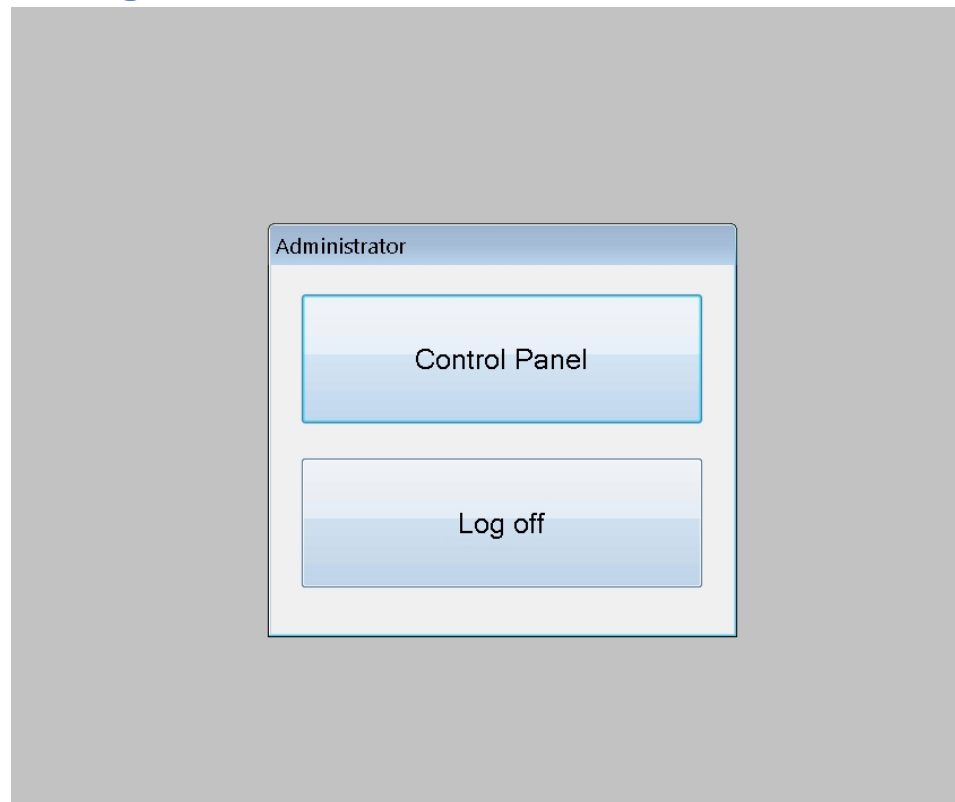
PS C:\Windows\system32> exit
C:\Windows\system32>_
```


10. Confirm Print Spooler service is disabled

Go into the Control Panel and select Administrative Tools -> Services

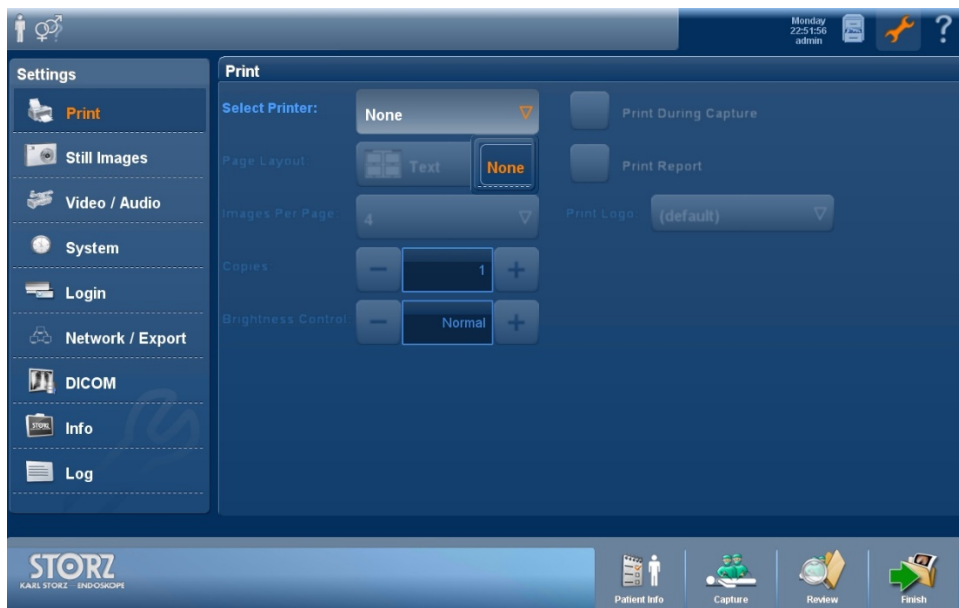


11. Log off and Go back to the AIDA User Interface



Impact of the workaround:

Disabling the Print Spooler service disables the ability to print both locally and remotely. After disabling the Print Spooler, no printers will be available for selection when displaying the 'Select Printer' option.



References:

1. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>
2. <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34527>