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

† 🗭				Monday 22:28:30 admin 🗧 🥠 ?
Settings	System			
ka Print	Hospital Name:			Show user on UI
间 Still Images	Surgical Feedback:	Thumbnail	\bigtriangledown	Audible Feedback
🐖 Video / Audio	Max Procedure Size:	No Limit	+	
System	Max Procedure in MB:			Enable Channel 2
💳 Login				
🖧 Network / Export	Procedure Deletion:	None		Admin Mode
🕅 ЫСОМ	Time Format:	24	\bigtriangledown	Calibrate Touchscreen
📼 Info	Set Time & Date			Reset Touchscreen
🔲 Log	Set keystore password			Mandatory Patient Info Fields
STORZ KARL STORZ - ENDOSINGH				Patient Info

2. Exit to the Windows OS



3. Select Control Panel

Administrator	
Control Panel	
Log off	
L	J

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



6. Get Print Spooler Status

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



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".



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.

🔚 Admir	nistrator: C:\Windo	ws\System32\cmd.exe - powershell 📃 🗌	
PS C:∖Wi	ndows\system32>	Get-Service -Name Spooler	^
Status 	Name	DisplayName	
Running	Spooler	Print Spooler	
PS C:\Wi PS C:\Wi	ndows\system32> ndows\system32>	Stop-Service -Name Spooler -Force	
PS C:∖Wi	ndows\system32>	Get-Service -Name Spooler	
Status	Name	DisplayName	
Stopped	Spooler	Print Spooler	
PS C:\Wi PS C:\Wi PS C:\Wi	ndows\system32> ndows\system32>	Set-Service -Name Spooler -StartupType Disabled	
P3 C:\W1	ndows\systemsz>	Get-Service -Name Spooler	
Status	Name	DisplayName	
Stopped	Spooler	Print Spooler	
PS C:∖Wi	ndows\system32>	_	
			~

9. Exit powershell and CMD

🔚 Admir	istrator: C:\Window	/s\System32\cmd.exe 📃 📃	×		
PS C:∖Wi	ndows\system32> (Get-Service -Name Spooler	•		
Status 	Name	DisplayName			
Running	Spooler	Print Spooler			
PS C:\Wi PS C:\Wi PS C:\Wi	ndows\system32> : ndows\system32>	Stop-Service -Name Spooler -Force			
PS C:\WI	ndows\system327 (der-Service -Name Spooler			
Status	Name	DisplayName			
Stopped	Spooler	Print Spooler			
PS C:∖Wi	ndows\system32> 3	Set-Service -Name Spooler -StartupType Disabled			
PS C:\W1 PS C:\Wi	ndows\system32> ndows\system32>	Get-Service -Name Spooler			
Status	Name	DisplayName			
Stopped	Spooler	Print Spooler			
PS C:∖Wi	ndows\system32>	exit			
C:\Windows\system32>					
			-		
PS C:\Wi Status Stopped PS C:\Wi C:\Windo	ndows\system32> (Name Spooler ndows\system32> (ws\system32> <u></u>	Get-Service -Name Spooler DisplayName Print Spooler exit	+		

10. Confirm Print Spooler service is disabled

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

Services						
File Action	View Help					
(= =) 🗔 🖸						
Services (Lo	Services (Local)					
	Print Spooler	Name	Description	Status	Startup Type	Log On As
	Description:	Plug and Play Pml Driver HP712	Enables a c	Started Started	Automatic Automatic	Local Syst
Loads files to memory for later printing		PNP-X IP Bus Enumerator	The PnP-X	ounted	Manual	Local Syst
		PORP Machine Name Publication Service Portable Device Enumerator Service	This service Enforces gr		Manual Manual	Local Serv Local Syst
		@ Power	Manages p	Started	Automatic	Local Syst
		🔍 Print Spooler	Loads files		Disabled	Local Syst
		Problem Reports and Solutions Control Panel Su	This service		Manual	Local Syst
		Program Compatibility Assistant Service	This service	Started	Automatic	Local Syst
		Protected Storage	Provides pr		Manual	Local Syst
		Quality Windows Audio Video Experience	Quality Wi		Manual	Local Serv
		Realtemp			Disabled	Local Syst
		RealTempService		Started	Automatic	Local Syst
		Remote Desktop Configuration	Remote De	Started	Manual	Local Syst
		Remote Desktop Services	Allows user	Started	Manual	Network S
		@ Remote Desiston Services LiserMode Port Redirec	∆llows the	Started	Manual	Local Svet

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

Administra	tor	
	Control Panel	
	Log off	

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.

† 🗭					Monday 22:51:56 admin 🔄 🥕 ?
Settings	Print				
ka Print	Select Printer:	None	V		
间 Still Images			None		
🐖 Video / Audio		4	 V P		
System					
🔜 Login					
🖧 Network / Export		Norma	· +		
🕅 ЫСОМ					
📠 Info					
Log					
				Patient Info	Review Finish

References:

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