

Fix Print Spooler Vulnerability using CB2103

In this post, I am going to use the script shared by MVP to fix above issue with DC and Print Servers within the lab. Microsoft recently shared the info about Print Spooler vulnerability via CVE 2021 34527 – <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527> -

Mitigations

To reduce the attack surface and as an alternative to disabling printing, check membership and nested group membership in the groups listed below. Attempt to reduce membership as much as possible, or completely empty the groups where possible. Due to legacy configurations and backwards compatibility, some of these groups may contain Authenticated Users or Domain Users, which would allow anyone in the domain to exploit the domain controller.

- Administrators
- Domain Controllers
- Read Only Domain Controllers
- Enterprise Read Only Domain Controllers
- Certificate Admins
- Schema Admins
- Enterprise Admins
- Group Policy Admins
- Power Users
- System Operators
- Print Operators
- Backup Operators
- RAS Servers
- Pre-Windows 2000 Compatible Access
- Network Configuration Operators Group Object
- Cryptographic Operators Group Object
- Local account and member of Administrators group

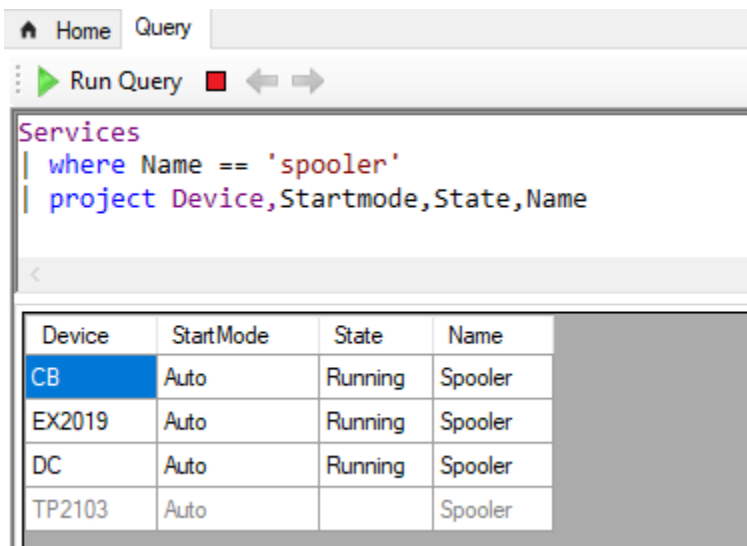
To mitigate, I am going to use the script. Following will the action plan:

1. Identify systems running print spooler using CMPivot
2. Stop and Disable print spooler service using new script
3. Enabling print spooler at Startup – if you need this to be running

Identify the system running print spooler - Open the Console – Device Collections – Start CMPivot and run this script. I have 4 systems running print spooler service.

Services

```
| where Name == 'spooler'  
| project Device,Startmode,State,Name
```




The screenshot shows a query console interface with a 'Query' tab selected. Below the query input, there is a 'Run Query' button. The query results are displayed in a table with the following columns: Device, StartMode, State, and Name.

Device	StartMode	State	Name
CB	Auto	Running	Spooler
EX2019	Auto	Running	Spooler
DC	Auto	Running	Spooler
TP2103	Auto		Spooler

Stop and Disable spooler service – Open Console – Go to Software Library – Scripts – Create Script

Create Script ✕

 Script Details

Script Details

- Summary
- Progress
- Completion

Specify script details

Specify the script to be executed on client devices.


Script name:

Script language:

Script:


```
3 Disable Print Spooler Service
4 .DESCRIPTION
5 Disable Print Spooler Service to mitigate the Windows
6 https://msrc.microsoft.com/update-guide/vulnerability
7 .NOTES
8 03.07.2021, v1.0.0, alex verboon
9 #>
10 Begin{
11     $PrintSpoolerState = (Get-Service -Name Spooler).S
12     $PrintSpoolStartMode = (Get-Service -Name Spooler).
13 }
14 Process{
15     If ($PrintSpoolerState -ne "Stopped"){
16         Write-host "Print Spooler is not stopped, stoppi
17         Stop-Service -Name Spooler -Force
18     }
19
20     If ($PrintSpoolStartMode -ne "Disabled"){
21         Write-host "Print Spooler is not disabled, disab
22         Set-Service -Name Spooler -StartupType Disabled
23     }
24 }
25 End{}
```

Create Script ✕

 Completion

Script Details

- Summary
- Progress
- Completion**

 The task "Create Script" completed successfully

Details:

Script details

Script Name: Print Spooler Stop Disable
Script Type: PowerShell

To exit the wizard, click Close.

Approve the script and run it.

Overview ▶ Scripts

< Scripts 7 items

Search

Name	Version	Author	Type	Approval State	Approver
Print Spooler Stop Disable	1	RAMLAN\Administrator	PowerShell	Approved	RAMLAN\Administrator

We are ready to run the script for device collections – Go to Device Collections – Run Script

Run Script

Run Script

Run Script

Summary

Select script to run

Script Status Monitoring

Select script to run

Choose a script to deploy to the selected resource. Only approved scripts are listed.

Filter...

Script Name	Script Type	Script GUID
001 Update User GPO	PowerShell	8EB09350-717B-4...
Capture Logs	PowerShell	9DD8C7DF-3659-4...
Configure Edge Auto Update	PowerShell	1463F5D2-E7C2-4...
GetNetFrameworkVersion	PowerShell	5453F733-A86E-4...
LAR Reset	PowerShell	76975268-A928-4...
OG	PowerShell	054F537A-24D5-4...
Print Spooler Stop Disable	PowerShell	811E26AA-605C-4...

Run Script

Script Status Monitoring

Run Script

Summary

Select script to run

Script Status Monitoring

Script status

Script completed on 3 of 4 clients.

Script Output

Bar Chart

Copy

Print Spooler is not stopped. ...

Client Count

Script Details | Summary | Run Details

You can also view script status in the monitoring workspace in the script status node.

< Previous | Next > | Summary | Close

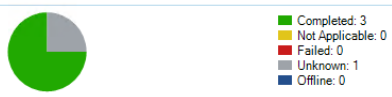
You can check the status under Monitoring – Script Status

Print Spooler Stop Disable

General

Script Name: Print Spooler Stop Disable
Script GUID: 811E26AA-605C-4COD-9E89-7F72496AD40E
Collection ID: SMSDM003
Last Update Time: 04-Jul-2021 11:10 AM
Total Clients: 4
Overall Script Execution State: Succeeded

Script Completion



Completed: 3
Not Applicable: 0
Failed: 0
Unknown: 1
Offline: 0

Now check the status again – Device Collection – CMPivot – The spooler is stopped

Home Query

Run Query

```
Services  
| where Name == 'spooler'  
| project Device,Startmode,State,Name
```

Device	StartMode	State	Name
EX2019	Disabled	Stopped	Spooler
CB	Disabled	Stopped	Spooler
DC	Disabled	Stopped	Spooler
TP2103	Auto		Spooler

If you want to rollback and want spooler to be running. Use this script

Create Script

Script Details

Script Details

Summary
Progress
Completion

Specify script details

Specify the script to be executed on client devices.

Script name: Print Spooler Start


Script language: PowerShell

Script: Import Clear

```
3 Enable Print Spooler Service  
4 .DESCRIPTION  
5 Enable Print Spooler Service  
6 .NOTES  
7 03.07.2021, v1.0.0, alex verboon  
8 #>  
9 Begin{  
10 $PrintSpoolerState = (Get-Service -Name Spooler).S  
11 $PrintSpoolStartMode = (Get-Service -Name Spooler).  
12 }  
13 Process{  
14  
15 If ($PrintSpoolStartMode -ne "Automatic"){  
16 Write-host "Print Spooler is not set to autostar  
17 Set-Service -Name Spooler -StartupType Automatic  
18 }  
19  
20 If ($PrintSpoolerState -ne "Running"){  
21 Write-host "Print Spooler is stopped, starting i  
22 Start-Service -Name Spooler  
23 }  
24 }  
25 End{}
```

< Previous Next > Summary Cancel

Create Script ✕

 **Completion**

Script Details

Summary

Progress

Completion

✔

The task "Create Script" completed successfully

Details:

Script details

Script Name: Print Spooler Start
Script Type: PowerShell

To exit the wizard, click Close.

< Previous
Next >
Summary
Close

Approve the script and run it.


Scripts 8 items

Search

Name	Version	Author	Type	Approval State	Approver	Approver Comment
Print Spooler Start	1	RAMLAN\Administrator	PowerShell	Waiting for approval		

Back to Device Collection – Run Script – Select Print Spooler Start

Run Script ✕

 **Script Status Monitoring**

Run Script

Summary

Select script to run

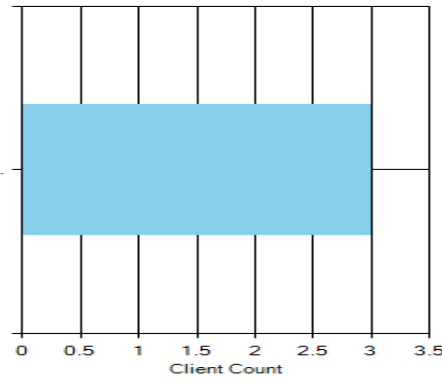
Script Status Monitoring

Script status

Script completed on 3 of 4 clients.

Script Output Bar Chart Copy

Print Spooler is not set to au...



Client Count

Script Details | Summary | Run Details

You can also view script status in the monitoring workspace in the script status node.

< Previous
Next >
Summary
Close

Print Spooler Start

General

Script Name: Print Spooler Start
Script GUID: 6489DB42-5A1C-4F64-8009-0D168E1FC190
Collection ID: SMSDM003
Last Update Time: 04-Jul-2021 11:18 AM
Total Clients: 4
Overall Script Execution State: Succeeded

Script Completion



Completed: 3
Not Applicable: 0
Failed: 0
Unknown: 1
Offline: 0

Device	StartMode	State	Name
CB	Auto	Running	Spooler
EX2019	Auto	Running	Spooler
DC	Auto	Running	Spooler
TP2103	Auto	Running	Spooler

Scripts Used Are:

Check Spooler Status - CMPivot

Services

```
| where Name == 'spooler'  
| project Device, Startmode, State, Name
```

Stop and Disable Spooler - Script

<#

.Synopsis

Disable Print Spooler Service

.DESCRIPTION

Disable Print Spooler Service to mitigate the Windows Print Spooler Remote Code Execution Vulnerability

<https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>

.NOTES

03.07.2021, v1.0.0, alex verboon

#>

Begin{

```
$PrintSpoolerState = (Get-Service -Name Spooler).Status
```

```
$PrintSpoolStartMode = (Get-Service -Name Spooler).StartType
```

}

Process{

```
If ($PrintSpoolerState -ne "Stopped"){
```

```
Write-host "Print Spooler is not stopped, stopping it now"
```

```
Stop-Service -Name Spooler -Force
```

```
}
```

```
If ($PrintSpoolStartMode -ne "Disabled"){
```

```
Write-host "Print Spooler is not disabled, disabling it now"
```

```
Set-Service -Name Spooler -StartupType Disabled
```

```
}
```

}

End{}

Start Spooler – Script

<#

.Synopsis

Enable Print Spooler Service

.DESCRIPTION

Enable Print Spooler Service

.NOTES

03.07.2021, v1.0.0, alex verboon

#>

Begin{

 \$PrintSpoolerState = (Get-Service -Name Spooler).Status

 \$PrintSpoolStartMode = (Get-Service -Name Spooler).StartType

}

Process{

 If (\$PrintSpoolStartMode -ne "Automatic"){

 Write-host "Print Spooler is not set to autostart, configuring that now"

 Set-Service -Name Spooler -StartupType Automatic

 }

 If (\$PrintSpoolerState -ne "Running"){

 Write-host "Print Spooler is stopped, starting it now"

 Start-Service -Name Spooler

 }

}

End{}