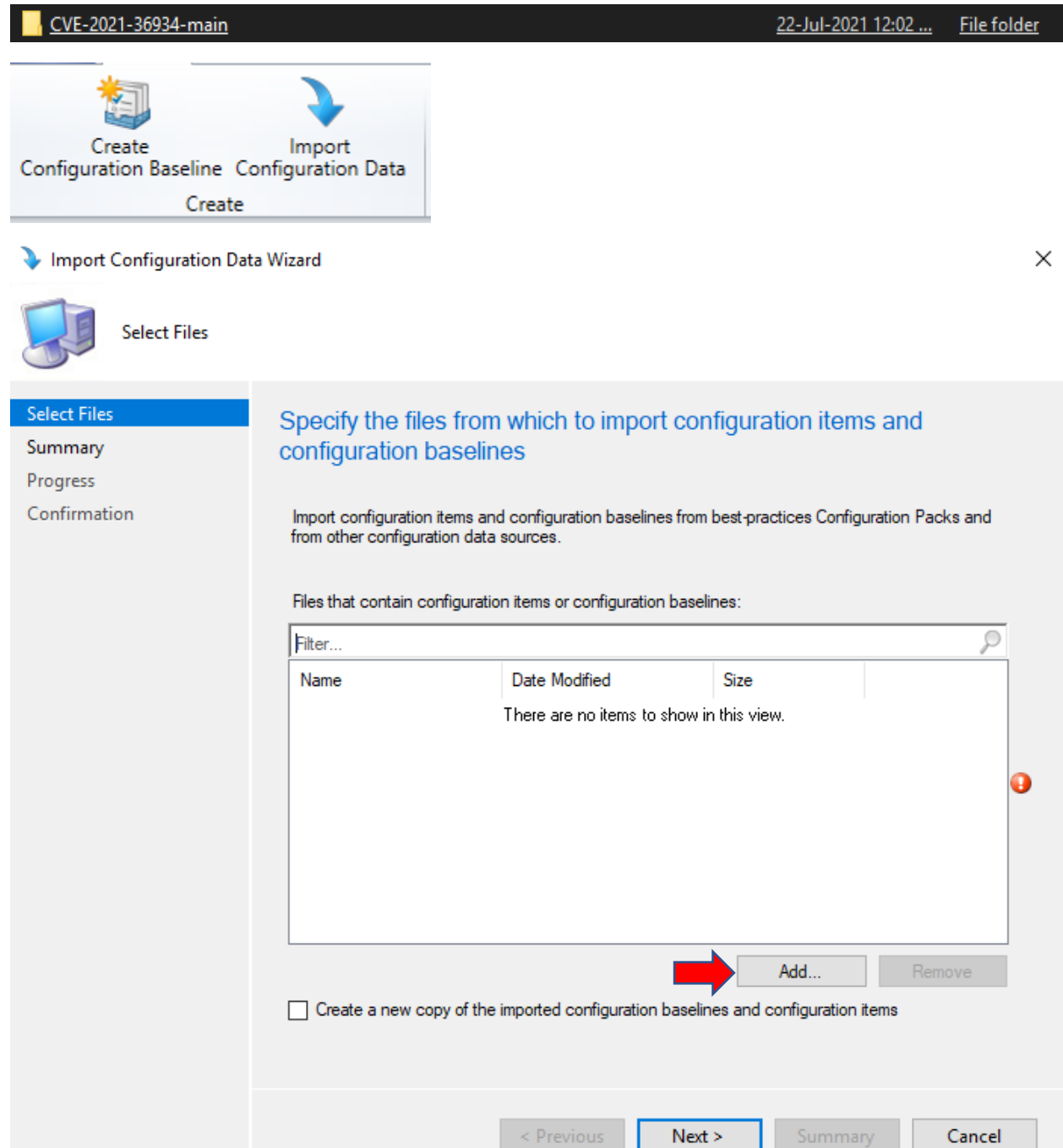
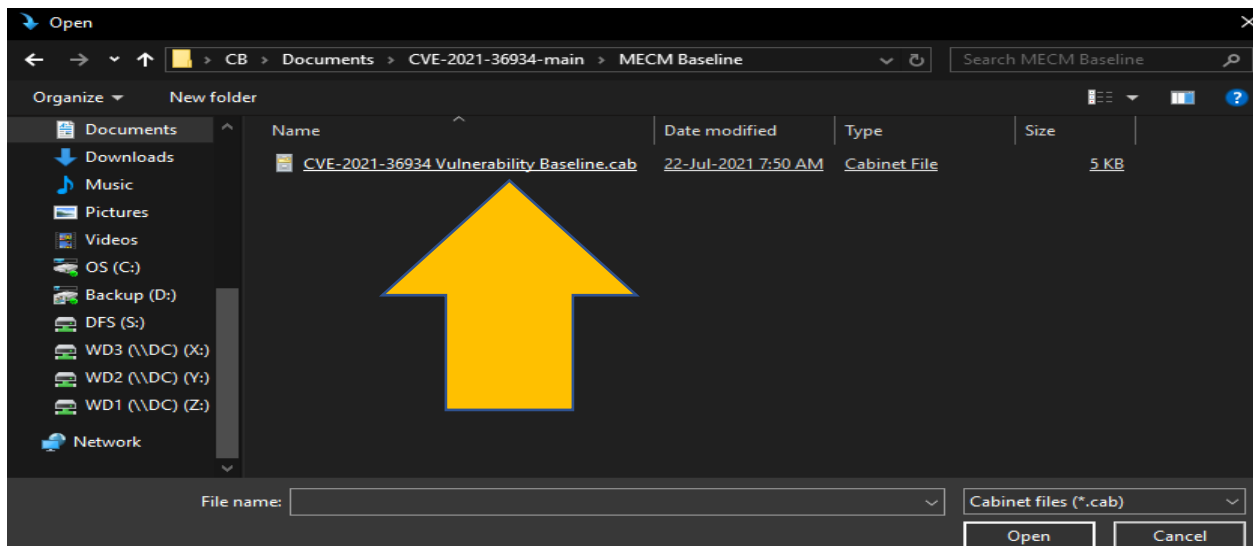


## CVE 2021 – 36934 – PowerShell Fix for MEMCM with Baseline – Elevation Vulnerability

I was able to get hold of MEM Baseline & Configuration Item cab file and PowerShell script to fix above vulnerability - <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36934> - You can deploy this to Win 10 collection only. Do not use it for File Server or Windows Server systems.

Copy the folder to the server and start the process by importing Configuration Data.





### Configuration Manager



The publisher of CVE-2021-36934 Vulnerability Baseline.cab file could not be verified. Are you sure that you want to import this file?

Yes

No

### Import Configuration Data Wizard



#### Select Files

#### Select Files

Summary

Progress

Confirmation

### Specify the files from which to import configuration items and configuration baselines

Import configuration items and configuration baselines from best-practices Configuration Packs and from other configuration data sources.

Files that contain configuration items or configuration baselines:

Filter...			
Name	Date Modified	Size	
CVE-2021-36934 Vulnera...	22-Jul-2021 7:50:50 AM	4.37 KB	

Add...

Remove

☐ Create a new copy of the imported configuration baselines and configuration items

< Previous

Next >

Summary

Cancel

## Import Configuration Data Wizard



### Summary

Select Files

Summary

Progress

Confirmation

### Confirm the configuration data to be imported:

The wizard will import the following configuration data.

Details:

- Configuration Baselines (1)
  - CVE-2021-36934
- Configuration Items (1)
  - CVE-2021-36934

To change these settings, click Previous. To apply the settings, click Next.

< Previous

Next >

Summary

Cancel

## Import Configuration Data Wizard



### Confirmation

Select Files

Summary

Progress

Confirmation

### Completing the Import Configuration Data Wizard

You have successfully completed the Import Configuration Data Wizard with the following details.

Details:

- Configuration Baselines (1)
  - CVE-2021-36934 [Success]
- Configuration Items (1)
  - CVE-2021-36934 [Success]

To close this wizard, click Close.

< Previous

Next >

Summary

Close

Below are Configuration Baseline and Configuration Item.

Overview

Compliance Settings

Configuration Baselines

Configuration Baselines 9 items

Search

Icon	Name	Status	Deployed	User Setting	Date Modified	Compliance Count	Noncompliance Count	Failure Count	Modified By
	CVE-2021-36934	Enabled	No	No	22-Jul-2021 12:06...	0	0	0	RAMLAN...

Overview

Compliance Settings

Configuration Items

Configuration Items 22 items

Search

Icon	Name	Type	Device Type	Revision	Child	Relationships	User Setting	Date Modified
	CVE-2021-36934	Operating System	Windows	1	No	Yes	No	22-Jul-2021 12:06 PM

We can deploy to Windows 10 collection only.

The screenshot shows the SCCM console interface. At the top, the 'Deploy' button is highlighted with a red box. Below it, the 'Configuration Baselines' section shows a table with one item: CVE-2021-36934, which is Enabled, Not Deployed, and has a User Setting of No. The date modified is 22-Jul-2021 12:06...

The 'Deploy Configuration Baselines' dialog box is open, showing the selection of configuration baselines. The 'Available configuration baselines' list includes 'CB - Office Activation', '1B: CustomerReady\_ESU - Windows 7 - K...', and '2: CustomerReady\_ESU - Windows 7/Wi...'. The 'Selected configuration baselines' list contains 'CVE-2021-36934'. The 'Remediate noncompliant rules when supported' checkbox is checked, and the 'Generate an alert' checkbox is also checked. The 'When compliance is below' is set to 90%, and the 'Date and time' is set to 22-Jul-2021 12:17 PM. The 'Generate System Center Operations Manager alert' checkbox is unchecked.

The 'Select the collection for this configuration baseline deployment' section shows the 'Collection' dropdown set to 'Win 10'. The 'Schedule' section shows the 'Simple schedule' selected, with 'Run every' set to 7 days. The 'Customize...' button is visible.

The 'OK' and 'Cancel' buttons are at the bottom of the dialog box.

Below the dialog box, a table shows the deployment status of the configuration baseline:

Icon	Collection	Compliance %	Deployment Start Time	Action
	Win 10	0.0	22-Jul-2021 12:19 PM	Remediate

You can sit back and let the baseline do its job.

<https://github.com/tda90/CVE-2021-36934> - Here is the download link for CB & CI.

Thanks

Ram Lan

22<sup>nd</sup> Jul 2021