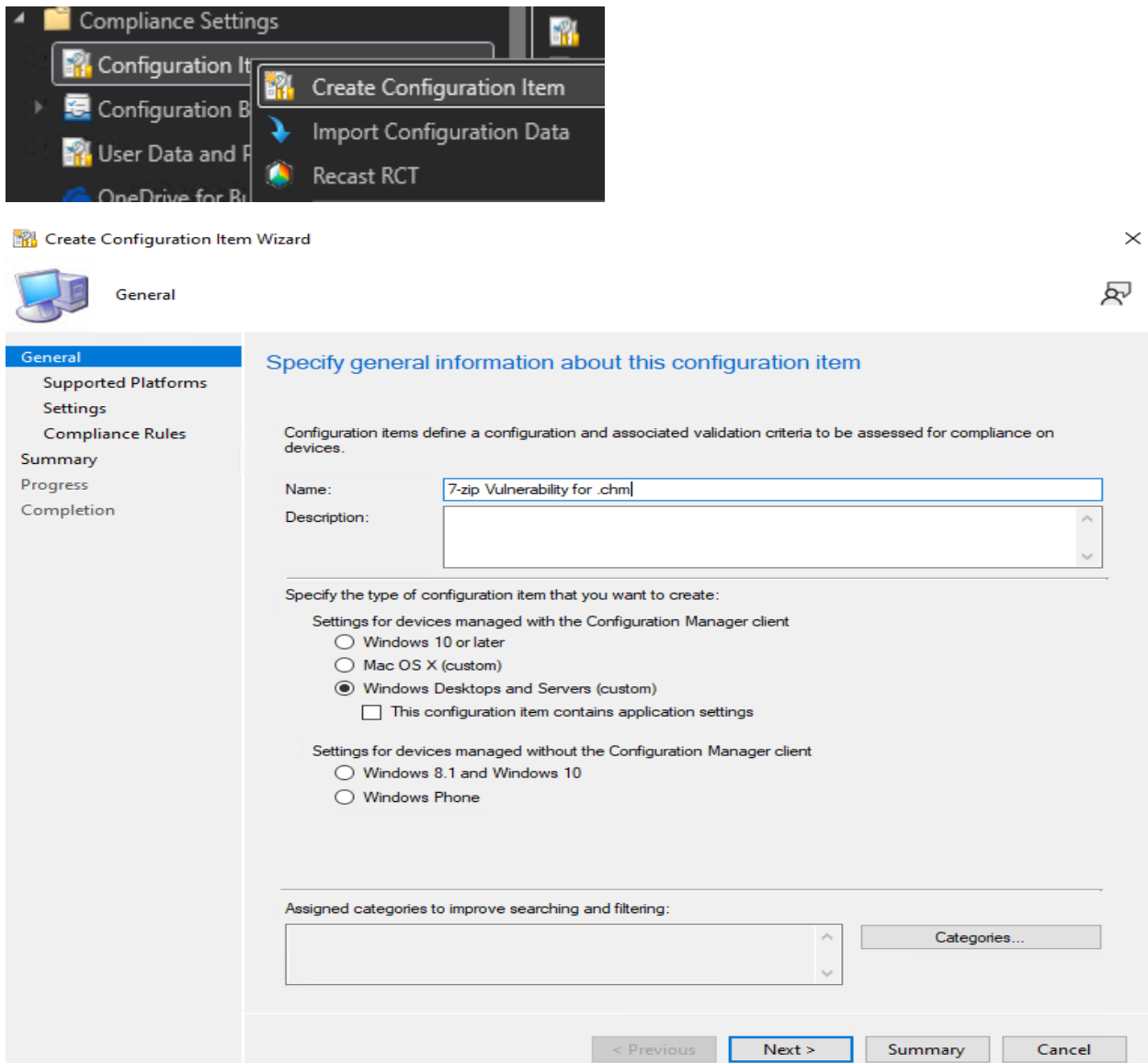


Remediating CVE-2022-29072 for 7-zip Windows Privilege Escalation Vulnerability

In this post, I am going to create CI and CB within CB2203 to fix 7-zip vulnerability for x64 version. Below are the details.

At present, 7-Zip has not released a security update to address this vulnerability, which means that all current versions of 21.07 are vulnerable. Luckily there is a workaround available and through this blog, I will cover the remediation steps of implementing this workaround using ConfigMgr.

1. On the MECM console, navigate to `\Assets and Compliance\Overview\Compliance Settings\Configuration Items`.
2. Right click and select *Create Configuration Item*.
3. Configure the settings as shown below.



The screenshot shows the 'Create Configuration Item Wizard' dialog box in the MECM console. The wizard is in the 'General' tab, and the 'Name' field is filled with '7-zip Vulnerability for .chm'. The 'Description' field is empty. The 'Specify the type of configuration item that you want to create:' section has 'Windows Desktops and Servers (custom)' selected. The 'Assigned categories to improve searching and filtering:' section is empty.

General

Specify general information about this configuration item

Configuration items define a configuration and associated validation criteria to be assessed for compliance on devices.

Name:

Description:

Specify the type of configuration item that you want to create:

Settings for devices managed with the Configuration Manager client

- Windows 10 or later
- Mac OS X (custom)
- Windows Desktops and Servers (custom)
 - This configuration item contains application settings

Settings for devices managed without the Configuration Manager client

- Windows 8.1 and Windows 10
- Windows Phone

Assigned categories to improve searching and filtering:

< Previous **Next >** Summary Cancel



General

Supported Platforms

Settings

Compliance Rules

Summary

Progress

Completion

Specify the client operating systems that will assess this configuration item for compliance

Select the versions of Windows that will assess this configuration item for compliance:

Select all

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows 2003
- Windows 2008
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Embedded
- Windows Server 2019
- Windows 11
- Windows Server 2022

Specify the version of Windows manually:

Add...

< Previous **Next >** Summary Cancel



General

Supported Platforms

Settings

Compliance Rules

Summary

Progress

Completion

Specify settings for this operating system

Use settings to represent business or technical conditions to assess for compliance on client devices. The following settings are associated with this configuration item.

Filter...

Name	Setting Type	Inherited	User Setting
There are no items to show in this view.			



New... Edit... Delete

< Previous **Next >** Summary Cancel

Create Setting ✕

General **Compliance Rules**

Specify details about this setting that represents a business or technical condition to assess for compliance on client devices.

Name:



Description:

Setting type:

Data type:


Discovery script

Specify the script to find and return the value to be assessed for compliance on client devices. Use the echo command to return the script value to Configuration Manager.

  Script status: No script specified.

Remediation script (optional)

Specify the script to remediate noncompliant setting values found on client devices. Configuration Manager passes the noncompliant value to the script as a parameter.

 Script status: No script specified.

Run scripts by using the logged on user credentials

Run scripts by using the 32-bit scripting host on 64-bit devices

DETECTION SCRIPT

Edit Discovery Script ✕

Specify the script to find and return the value to be assessed for compliance on client devices. Use the echo command to return the script value to Configuration Manager.

Script language:

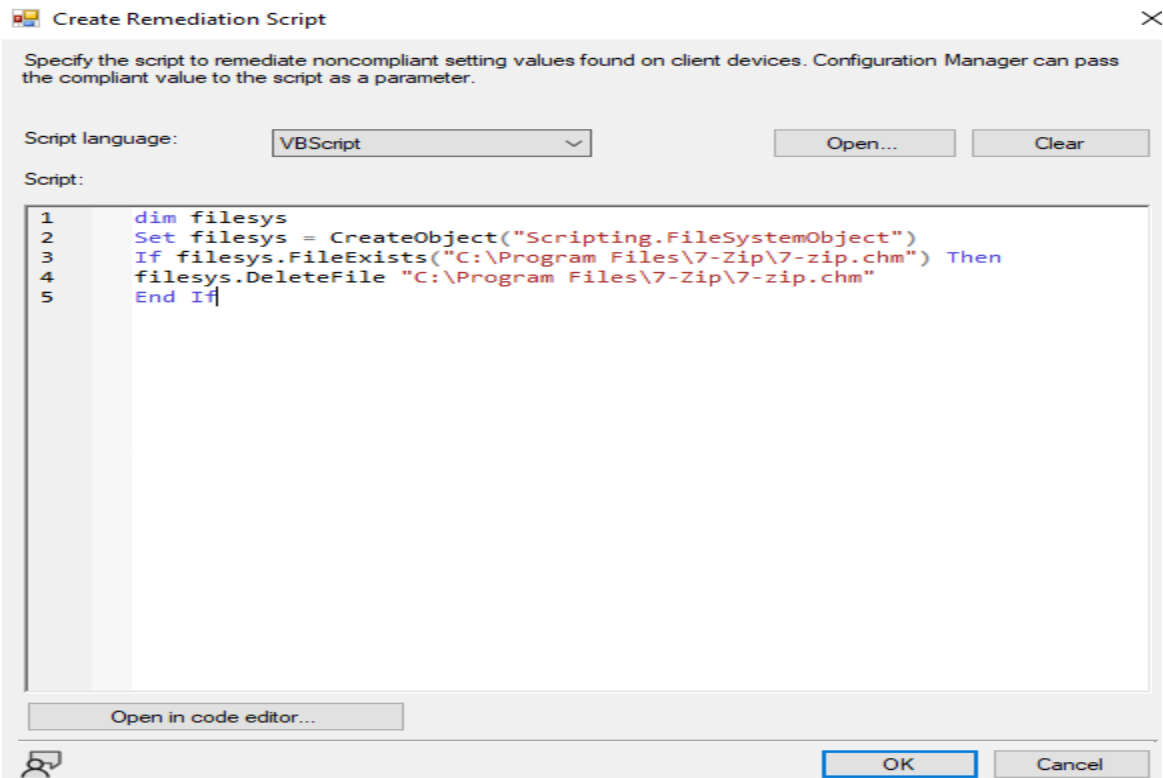
Script:

```

1  dim filesystem
2  Set filesystem = CreateObject("Scripting.FileSystemObject")
3  If filesystem.FileExists("C:\Program Files\7-Zip\7-zip.chm") Then
4  WScript.Echo "File exists"
5  Else
6  WScript.Echo "File does not exist"
7  End If

```

REMEDIATION SCRIPT:

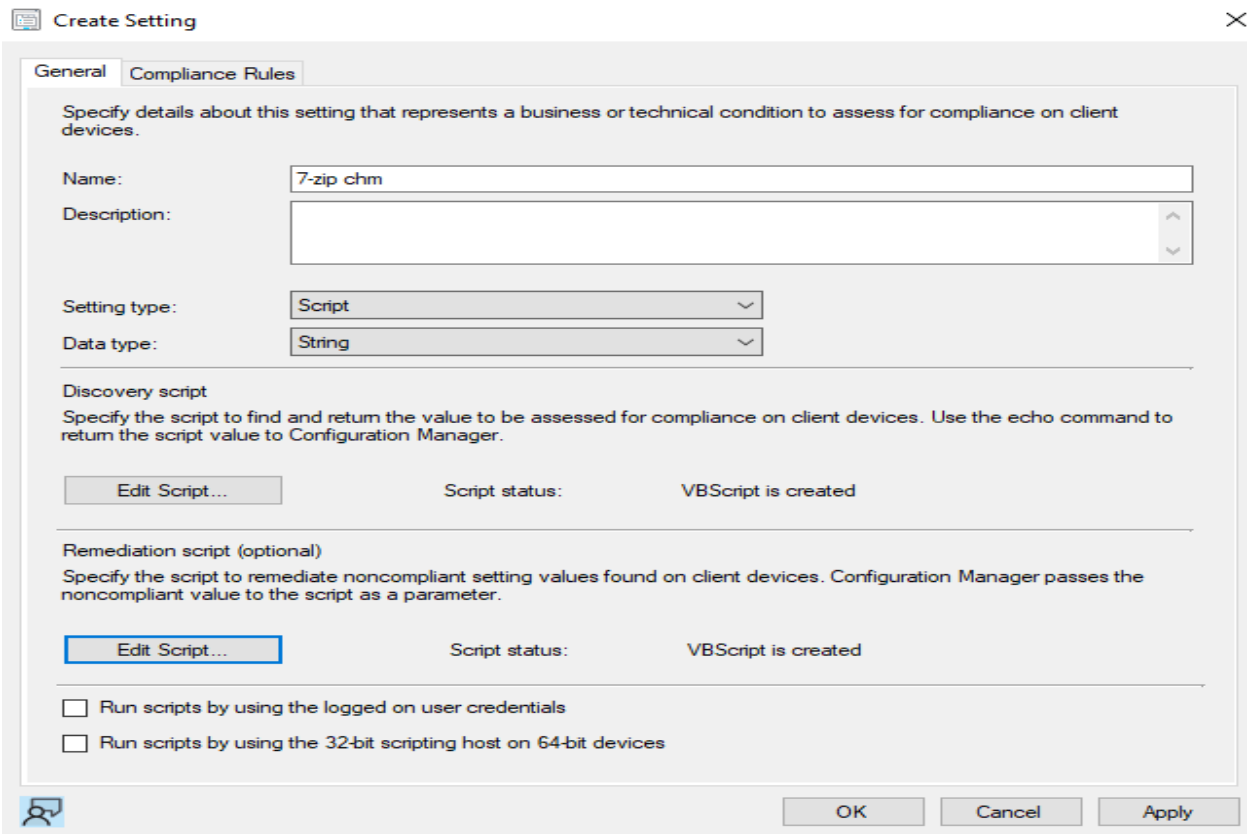
 Create Remediation Script

Specify the script to remediate noncompliant setting values found on client devices. Configuration Manager can pass the compliant value to the script as a parameter.

Script language:

Script:

```
1 dim filesystems
2 Set filesystems = CreateObject("Scripting.FileSystemObject")
3 If filesystems.FileExists("C:\Program Files\7-Zip\7-zip.chm") Then
4 filesystems.DeleteFile "C:\Program Files\7-Zip\7-zip.chm"
5 End If
```

 Create Setting

General Compliance Rules

Specify details about this setting that represents a business or technical condition to assess for compliance on client devices.

Name:

Description:

Setting type:

Data type:

Discovery script

Specify the script to find and return the value to be assessed for compliance on client devices. Use the echo command to return the script value to Configuration Manager.

Script status: VBScript is created

Remediation script (optional)

Specify the script to remediate noncompliant setting values found on client devices. Configuration Manager passes the noncompliant value to the script as a parameter.

Script status: VBScript is created

Run scripts by using the logged on user credentials

Run scripts by using the 32-bit scripting host on 64-bit devices



- General
- Supported Platforms
- Settings**
- Compliance Rules
- Summary
- Progress
- Completion

Specify settings for this operating system

Use settings to represent business or technical conditions to assess for compliance on client devices. The following settings are associated with this configuration item.

Filter...

Name	Setting Type	Inherited	User Setting
7-zip chm	Script	No	No



- General
- Supported Platforms
- Settings
- Compliance Rules**
- Summary
- Progress
- Completion

Specify compliance rules for this operating system

Use compliance rules to specify the conditions that make a configuration item setting compliant on client devices. The following compliance rules are associated with this configuration item.

Track remediation history when supported

Name	Setting Name	CI Name	Condition	Severity	Remediate	R
There are no items to show in this view.						



Specify rules to define compliance conditions for this setting

Name:

Description:

Selected setting:

Rule type:

The setting must comply with the following rule:
 Operator:
 For the following values:

- Run the specified remediation script when this setting is noncompliant
- Report noncompliance if this setting instance is not found

Noncompliance severity for reports:

- General
- Supported Platforms
- Settings
- Compliance Rules**
- Summary
- Progress
- Completion

Specify compliance rules for this operating system

Use compliance rules to specify the conditions that make a configuration item setting compliant on client devices. The following compliance rules are associated with this configuration item.

- Track remediation history when supported

Name	Setting Name	CI Name	Condition	Severity	Remediate	R
File does not exist	7-zip chm	7-zip Vulner...	Equals File d...	Critical	Yes	



Summary



General

Supported Platforms

Settings

Compliance Rules

Summary

Progress

Completion

The wizard will create an operating system configuration item with the following settings

Details:

The wizard will create an operating system configuration item with the following settings:

New operating system configuration item will be saved as:

- Name: 7-zip Vulnerability for .chm
- Description:
- Categories:

The following Windows versions are supported:

- All Windows client and server

The following compliance rules are added:

- File does not exist

The following settings are added:

- 7-zip chm

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

< Previous

Next >

Summary

Cancel



Completion



General

Supported Platforms

Settings

Compliance Rules

Summary

Progress

Completion



The task "Create Configuration Item Wizard" completed successfully

Details:

Success: The Create Configuration Item Wizard completed successfully.

New operating system configuration item will be saved as:

- Name: 7-zip Vulnerability for .chm
- Description:
- Categories:

The following Windows versions are supported:

- All Windows client and server

The following compliance rules are added:

- File does not exist

The following settings are added:

- 7-zip chm

To exit the wizard, click Close.

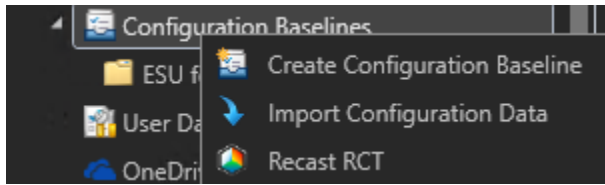
< Previous

Next >

Summary

Close

Now we have to create CB (Configuration Baselines)



Specify general information about this configuration baseline

Name: 7-zip for chm

Description:

Select the configuration data (configuration items, configuration baselines, and software updates) to be evaluated for compliance by this configuration baseline. This configuration baseline will be assessed as compliant if all the items specified are compliant. Optional items are evaluated only if the relevant application is present on the client devices.

Configuration data:

Filter...

Name	Type	Purpose	Revision
There are no items to show in this view.			

Add | Change Purpose | Change Revision | Remove

- Configuration Items
- Software Updates
- Configuration Baselines

Assigned categories to improve searching and filtering:

Categories...

OK Cancel

Add Configuration Items



Select the configuration items that you want to add to this configuration baseline

Available configuration items:

Name	Type	Latest Revision	Description
Check Client Boundary Groups	Operating System	Revision 1	
Check if file exists (Log4j)	Operating System	Revision 2	This CI checks for the exist
CI - DNS Server Vulnerability (CVE-2020-13...	Operating System	Revision 1	Workaround for wormable
CI - ESU - Server 2008 Status	Operating System	Revision 1	
CI - ESU - Windows 7 status	Operating System	Revision 2	
CustomerReady_ESU - Windows 7/Windo...	Operating System	Revision 7	install product key for ESU
CVE-2021-36934	Operating System	Revision 1	
ESU - Win7 - KB check - KB4474419 (SHA-2)	Operating System	Revision 6	checks for kb4474419, ES
ESU - Win7 - KB check - KB4490628 (ESU)	Operating System	Revision 5	checks for KB4490628, ES

Add

Remove

Configuration items that will be added to this configuration baseline:

Name	Type	Latest Revision	Description	Status
7-zip Vulnerability for	Operating System	Revision 1		Enabled



OK

Cancel

Create Configuration Baseline



Specify general information about this configuration baseline



Name:

7-zip for chm

Description:

Select the configuration data (configuration items, configuration baselines, and software updates) to be evaluated for compliance by this configuration baseline. This configuration baseline will be assessed as compliant if all the items specified are compliant. Optional items are evaluated only if the relevant application is present on the client devices.

Configuration data:

Name	Type	Purpose	Revision
7-zip Vulnerability for .chm	Operating System	Required	Latest

Add

Change Purpose

Change Revision

Remove

Always apply this baseline even for co-managed clients

Evaluate this baseline as part of compliance policy assessment

Assigned categories to improve searching and filtering:

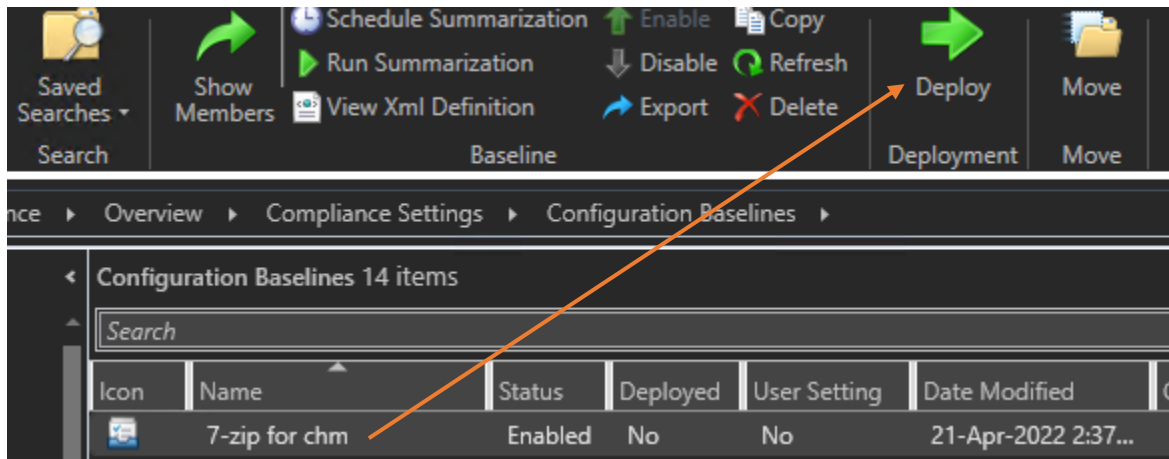
Categories...



OK

Cancel

Now deploy the CB



Deploy Configuration Baselines



Select the configuration baselines that you want to deploy to a collection

Available configuration baselines:

Filter...

- CB - Office Activation
- 1B: CustomerReady_ESU - Windows 7 - K
- 2: CustomerReady_ESU - Windows 7/Wi..

Add >
< Remove

Selected configuration baselines:

Filter...

- 7-zip for chm

- Remediate noncompliant rules when supported
 - Allow remediation outside the maintenance window
- Generate an alert:
 - When compliance is below: 90 %
 - Date and time: 22-Apr-2022 6:39 PM
 - Generate System Center Operations Manager alert

Select the collection for this configuration baseline deployment.

Collection: All Systems Browse...

Schedule

Specify the compliance evaluation schedule for this configuration baseline:

Simple schedule
Run every: 7 Days

Custom schedule
Occurs on 21-Apr-2022 3:40 PM Customize...



OK

Cancel

Custom Schedule ✕

Time
 Start:
 Coordinated Universal Time (UTC)

Recurrence pattern
 Configure the recurrence schedule.

None
 Monthly
 Weekly
 Custom interval

No recurrence. The scheduled event occurs once at the specified time.

Note: I will not recommend setting a recurrence schedule as the vulnerability may get fixed in future releases of 7-zip.

Configuration Baselines 14 items

Search

Icon	Name	Status	Deployed	User Setting	Date Modified	Compliance Count	Noncompliance Count	Failure Count	Modified By
	7-zip for chm	Enabled	Yes	No	21-Apr-2022 2:37...	0	0	0	RAMLAN...
	CB - Check client bound...	Enabled	Yes	No	17-Feb-2020 10:3...	9	0	0	RAMLAN...
	CB - DNS Server Vulner...	Enabled	Yes	No	15-Jul-2020 9:22 A...	3	0	0	RAMLAN...
	CB - ESU - Server 2008...	Enabled	No	No	11-May-2020 11:2...	0	0	0	RAMLAN...
	CB - ESU - Windows 7 a...	Enabled	Yes	No	11-May-2020 11:2...	0	0	0	RAMLAN...
	CB - Office Activation	Enabled	Yes	No	13-Sep-2019 9:57...	1	5	0	RAMLAN...
	CVE-2021-36934	Enabled	Yes	No	22-Jul-2021 12:06...	0	0	0	RAMLAN...
	HAFNIUM Exchange 2019	Enabled	Yes	No	22-Mar-2021 12:5...	0	1	0	RAMLAN...
	Log4j	Enabled	Yes	No	17-Dec-2021 11:3...	5	2	2	RAMLAN...
	LOG4J EXISTENCE TEST	Enabled	Yes	No	17-Dec-2021 11:5...	5	3	1	RAMLAN...
	LOG4J EXISTS	Enabled	Yes	No	17-Dec-2021 11:5...	7	2	0	RAMLAN...
	LOG4J HASH EVALUATI...	Enabled	Yes	No	17-Dec-2021 11:5...	7	0	2	RAMLAN...
	Microsoft Exchange Ser...	Enabled	Yes	No	22-Mar-2021 1:29...	0	1	0	RAMLAN...

7-zip for chm

Icon	Collection	Compliance %	Deployment Start Time	Action
	All Systems	0.0	21-Apr-2022 3:40 PM	Remediate

Configuration Items 27 items

Search

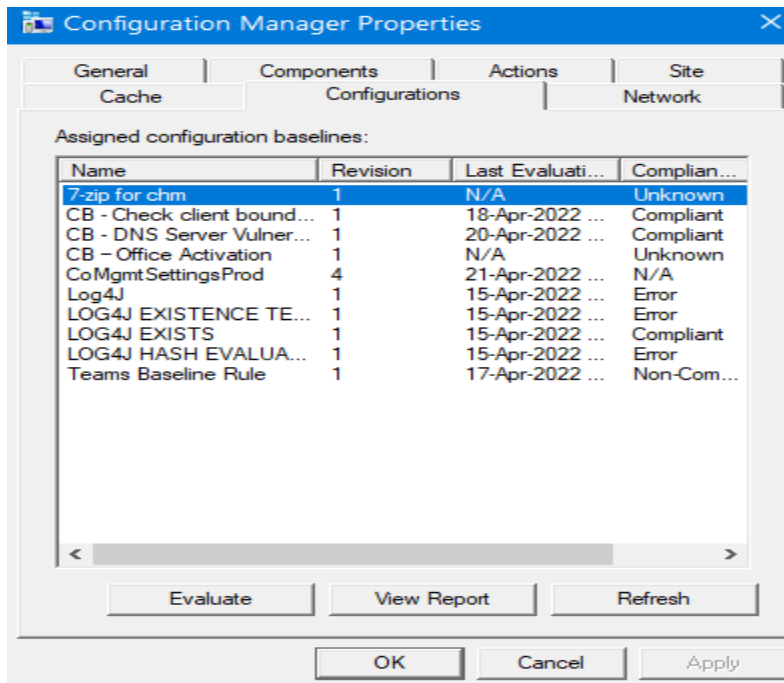
Icon	Name	Type	Device Type	Revision	Child	Relationships	User Setting	Date Modified
	7-zip Vulnerability for .chm	Operating Syst...	Windows	1	No	Yes	No	21-Apr-2022 2:34...
	Check Client Boundary Groups	Operating Syst...	Windows	1	No	Yes	No	17-Feb-2020 10:3...
	Check if file exists (Log4j)	Operating Syst...	Windows	2	No	Yes	No	17-Dec-2021 11:5...
	CI - DNS Server Vulnerability (CVE-2...	Operating Syst...	Windows	1	No	Yes	No	15-Jul-2020 9:22 A...
	CI - ESU - Server 2008 Status	Operating Syst...	Windows	1	No	Yes	No	11-May-2020 11:2...
	CI - ESU - Windows 7 status	Operating Syst...	Windows	2	No	Yes	No	11-May-2020 11:2...
	CustomerReady_ESU - Windows 7/...	Operating Syst...	Windows	7	No	Yes	No	04-Feb-2020 4:04...
	CVE-2021-36934	Operating Syst...	Windows	1	No	Yes	No	22-Jul-2021 12:06...
	ESU - Win7 - KB check - KB4474419...	Operating Syst...	Windows	6	No	Yes	No	04-Feb-2020 3:36...
	ESU - Win7 - KB check - KB4490628...	Operating Syst...	Windows	5	No	Yes	No	04-Feb-2020 3:36...
	ESU - Win7 - KB check - Multiple Cu...	Operating Syst...	Windows	4	No	Yes	No	04-Feb-2020 3:36...
	ESU - Win7 - KB check - Multiple Ser...	Operating Syst...	Windows	8	No	Yes	No	04-Feb-2020 3:36...
	ESU - WinServer 2008 R2 SP1 - KB c...	Operating Syst...	Windows	7	No	Yes	No	04-Feb-2020 3:36...

7-zip Vulnerability for .chm

Configuration Item Properties		Configuration Item Status	
Name:	7-zip Vulnerability for .chm	Relationships:	Yes
Type:	Operating System	User Setting:	No
Child:	No	Status:	Enabled
Revision:	1		
Date Created:	21-Apr-2022 2:34 PM		
Date Modified:	21-Apr-2022 2:34 PM		
Created By:	RAMLAN\Administrator		
Modified By:	RAMLAN\Administrator		
Device Type:	Windows		
Categories:			

We can check whether the remediation took place from Control Panel – Configuration Manager

Run Machine Policy and User Policy - Then check Configuration tab



In our case the remediation script status is UNKNOWN. I did set the script to run at 340pm. Maybe I will check tomorrow and the status should be COMPLIANT.

Conclusion

Until a fix is released, implementing the workaround seems like the only option.

Thanks

Ram

21st Apr 2022

SCRIPT: Detection x64 -

dim filesystems

Set filesystems = CreateObject("Scripting.FileSystemObject")

If filesystems.FileExists("C:\Program Files\7-Zip\7-zip.chm") Then

WScript.Echo "File exists"

Else

WScript.Echo "File does not exist"

End If

SCRIPT: Detection x86 -

```
dim filesystems
Set filesystems = CreateObject("Scripting.FileSystemObject")
If filesystems.FileExists("C:\Program Files (x86)\7-Zip\7-zip.chm") Then
WScript.Echo "File exists"
Else
WScript.Echo "File does not exist"
End If
```

SCRIPT: Remediation x64 -

```
dim filesystems
Set filesystems = CreateObject("Scripting.FileSystemObject")
If filesystems.FileExists("C:\Program Files\7-Zip\7-zip.chm") Then
filesystems.DeleteFile "C:\Program Files\7-Zip\7-zip.chm"
End If
```

SCRIPT: Remediation x86 -

```
dim filesystems
Set filesystems = CreateObject("Scripting.FileSystemObject")
If filesystems.FileExists("C:\Program Files (x86)\7-Zip\7-zip.chm") Then
filesystems.DeleteFile "C:\Program Files (x86)\7-Zip\7-zip.chm"
End If
```