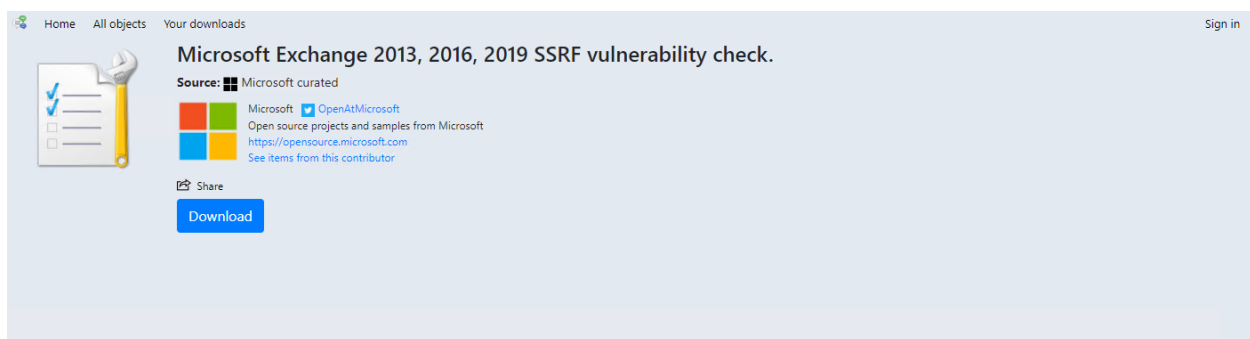
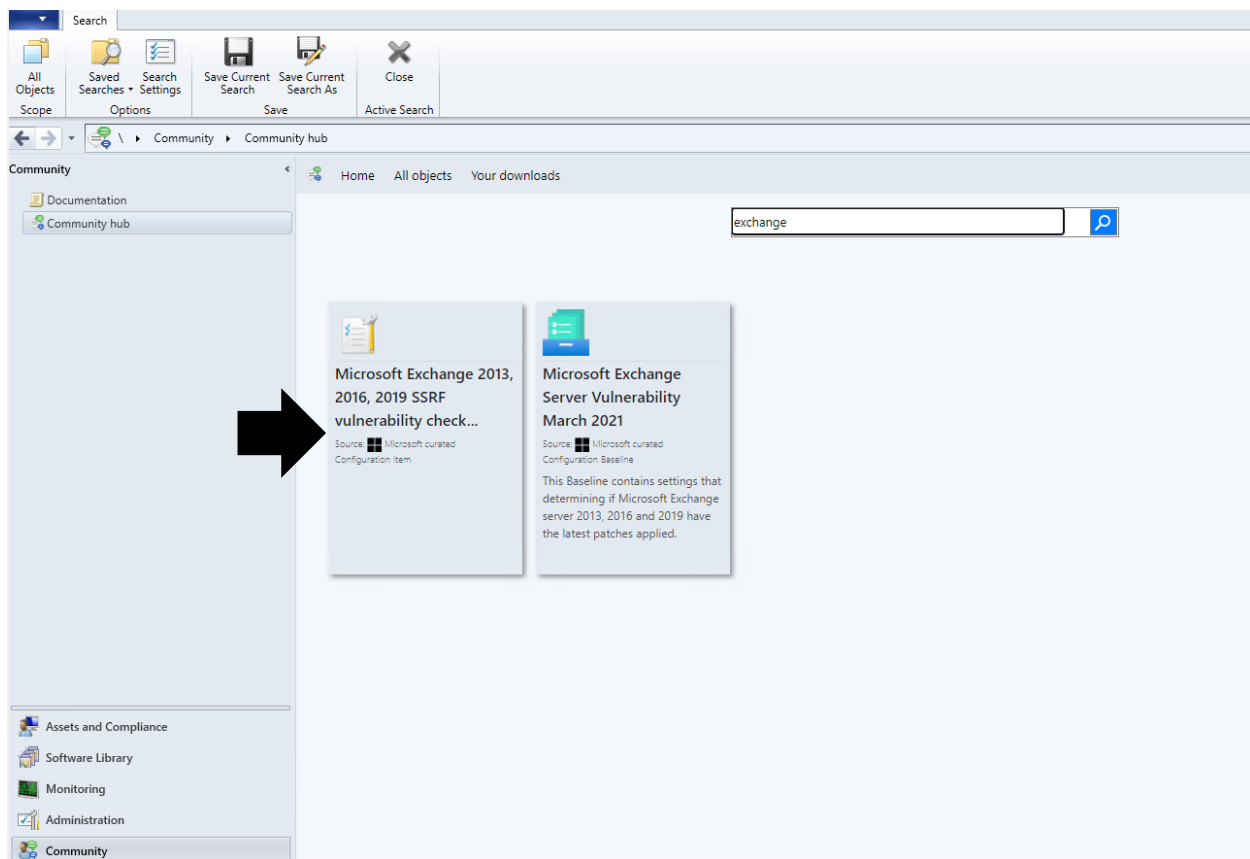


Community Hub Contribution to test and fix Exchange Server HAFNIUM

In this post, I will install Configuration Item (CI) contributed by configuration Manager community to test and fix Exchange Server. Within the lab, I am running Exchange Server 2019. I will use Current Branch 2010 to test and share the end result.



Overview [View Source](#)

Description:

Type: Configuration Item

Created by: Mark Silvey

Created date: 3/13/2021 12:38 PM


Changed date: 3/13/2021 6:39 PM

Disclaimer: Content stored within GitHub and accessed from the Community hub isn't supported by Microsoft. Microsoft doesn't validate content collected from or shared by the general community. GitHub is an external service subject to its own privacy and licensing terms. Your download and use of any files from GitHub here is subject to the license terms of those files provided on GitHub.


[GitHub Privacy Statement](#)


[GitHub Terms of Service](#)

Home All objects Your downloads Sign in




Microsoft Exchange 2013, 2016, 2019 SSRF vulnerability check.

Source:  Microsoft curated

 Open source projects and samples from Microsoft
<https://opensource.microsoft.com>
 See items from this contributor




Share

 This item was downloaded on 3/22/2021 12:04 PM

Download success!

Community hub

Home All objects Your downloads


Name	Download date	Downloaded by	Curation Status	Commit
 Configure Edge Auto Update	7/12/2020 11:35 AM	RAMLAN\yam	Curated	Commit information (external)
 Logical Disk per Device Chart	10/2/2020 10:50 AM	RAMLAN\anram	Curated	Commit information (external)
 Microsoft Exchange 2013, 2016, 2019 SSRF vulnerability check.	3/22/2021 12:04 PM	RAMLAN\Administrator	Curated	Commit information (external)

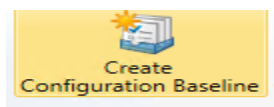
Here is our downloaded compliance item. We can create a baseline and deploy.

Assets and Compliance > Overview > Compliance Settings > Configuration Items

Configuration Items 20 items


Search

Icon	Name	Type	Device Type	Revision	Child	Relationships	User Setting	Date Modified
	Microsoft Exchange 2013, 2016, 2019 SSRF vulnerability check.	Application	Windows	7	No	No	No	22-Mar-2021 12:04 PM



Create Configuration Baseline

Specify general information about this configuration baseline

 Name:

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
There are no items to show in this view.			

- Configuration Items
- Software Updates for co-managed clients
- Configuration Baselines for compliance policy assessment

Assigned categories to improve searching and filtering:

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

Available configuration items:

Name	Type	Latest Revision	Description
ESU - WinServer 2008 SP2 - KB check - K...	Operating System	Revision 4	checks for kb4493730, ES...
ESU - WinServer 2008 SP2 - KB check - ...	Operating System	Revision 7	checks for Sept./Nov./De..
ESU - WinServer 2008/2008 R2 SP1 - KB ...	Operating System	Revision 7	checks for kb4474419, ES...
ESU - WinServer2008 R2 SP1 - KB check...	Operating System	Revision 5	checks for KB4490628, ES
ESU - WinServer2008 R2 SP1 - KB check...	Operating System	Revision 10	checks for KB4516655, KB
MS Teams Compliance Status	Operating System	Revision 1	
Office Activation Status	Operating System	Revision 1	
WVD Windows 10 Multi-Session	Operating System	Revision 1	

Add

Remove

Configuration items that will be added to this configuration baseline:

Name	Type	Latest Revision	Description	Status
Microsoft Exchange 2...	Application	Revision 7	This Configuration Item will ...	Enabled

OK

Cancel

Create Configuration Baseline

Specify general information about this configuration baseline



Name: HAFNIUM Exchange 2019

Description: This Baseline contains settings that determining if Microsoft Exchange server 2013, 2016 and 2019 have the latest patches applied.

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
Microsoft Exchange 2013, 2016, 2019 SSRF v...	Application	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:

"IT Infrastructure"

Categories...

OK

Cancel

Now we can deploy to Exchange Server collection and run the baseline.

The screenshot shows the Configuration Baselines console. The 'Deploy' button in the ribbon is highlighted with a black arrow. Below the ribbon, a table lists configuration baselines. The 'HAFNIUM Exchange 2019' baseline is selected, indicated by a black arrow pointing to its row.

Icon	Name	Status	Deployed	User Setting	Date Modified	Compliance Count	Noncompliance Count	Failure Count	Modified By
	CB - Check client boundary group	Enabled	Yes	No	17-Feb-2020 10:3...	18	0	0	RAMLAN...
	CB - DNS Server Vulnerability (CVE-2020-1350)	Enabled	Yes	No	15-Jul-2020 9:22 A...	4	0	0	RAMLAN...
	CB - ESU - Server 2008 Activation	Enabled	No	No	11-May-2020 11:2...	0	0	0	RAMLAN...
	CB - ESU - Windows 7 activation	Enabled	Yes	No	11-May-2020 11:2...	0	0	0	RAMLAN...
	CB - Office Activation	Enabled	Yes	No	13-Sep-2019 9:57...	5	7	1	RAMLAN...
	HAFNIUM Exchange 2019	Enabled	No	No	22-Mar-2021 12:5...	0	0	0	RAMLAN...

The screenshot shows the 'Deploy Configuration Baselines' dialog box. 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 'HAFNIUM Exchange 2019'. The 'Remediate noncompliant rules when supported' checkbox is unchecked. The 'Generate an alert' checkbox is also unchecked. The 'When compliance is below' dropdown is set to '90 %'. The 'Date and time' dropdown is set to '22-Mar-2021' and '12:50 PM'. The 'Generate System Center Operations Manager alert' checkbox is unchecked. The 'Collection' dropdown is set to 'EX2019'. The 'Schedule' section is set to 'Simple schedule' with 'Run every' set to '7' and 'Days' selected. The 'OK' and 'Cancel' buttons are visible at the bottom.

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

Available configuration baselines:

Selected configuration baselines:

Remediate noncompliant rules when supported

Generate an alert:

When compliance is below: 90 %

Date and time: 22-Mar-2021 12:50 PM

Generate System Center Operations Manager alert

Select the collection for this configuration baseline deployment.

Collection: EX2019

Schedule

Specify the compliance evaluation schedule for this configuration baseline:

Simple schedule

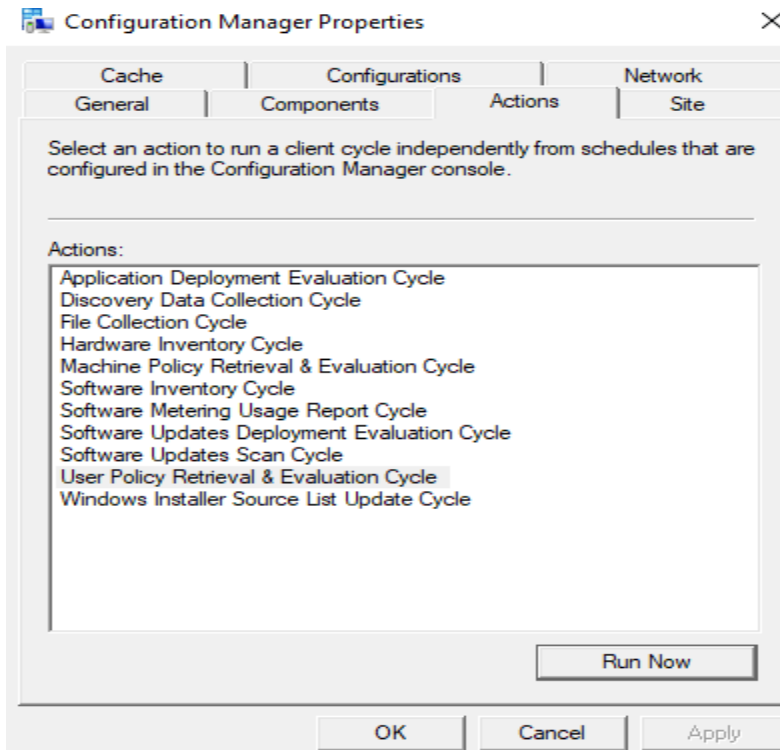
Run every: 7 Days

Custom schedule

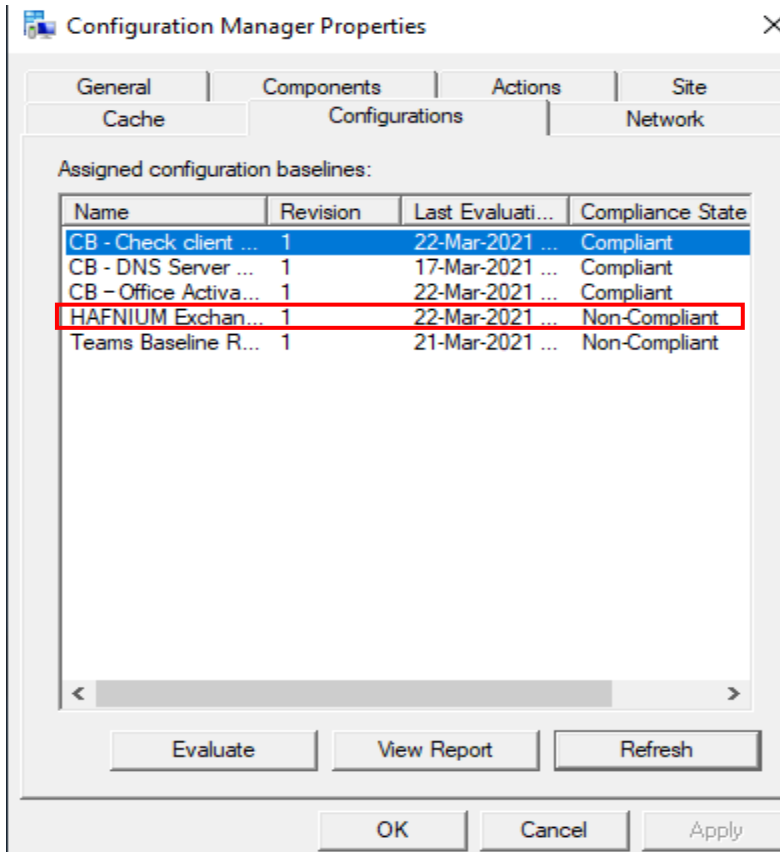
No custom schedule defined.

OK Cancel

Now run Machine and User policy.



From the screen shot the state is Non Compliant



Here is the report

Compliance Report

File Edit View Favorites Tools Help

Report View | Xml View

COMPUTER NAME: EX2019
 EVALUATION TIME: 22-Mar-2021 12:54:54 PM

BASELINE NAME: HAFNIUM Exchange 2019
 REVISION: 1

COMPLIANCE STATE: **Non-Compliant**
 NON-COMPLIANCE SEVERITY: **Critical**

DESCRIPTION: This Baseline contains settings that determining if Microsoft Exchange server 2013, 2016 and 2019 have the latest patches applied.

Summary:

Name	Revision	Type	Baseline Policy	Compliance State	Non-Compliance Severity	Discovery Failures	Non-Compliant Rules	Remediated Rules	Conflicting Rules
HAFNIUM Exchange 2019	1	Baseline		Non-Compliant	Critical	0	1	0	0
Microsoft Exchange 2013, 2016, 2019 SSRF vulner...	7	Application Configuration	Required	Non-Compliant	Critical	0	1	0	0

Details:

NAME: HAFNIUM Exchange 2019
 TYPE: Baseline
 REVISION: 1
 COMPLIANCE STATE: **Non-Compliant**
 NON-COMPLIANCE SEVERITY: **Critical**

DESCRIPTION: This Baseline contains settings that determining if Microsoft Exchange server 2013, 2016 and 2019 have the latest patches applied.

NAME: Microsoft Exchange 2013, 2016, 2019 SSRF vulnerability check.
 TYPE: Application Configuration
 REVISION: 7
 COMPLIANCE STATE: **Non-Compliant**
 NON-COMPLIANCE SEVERITY: **Critical**

DESCRIPTION: This Configuration Item will check if the following Microsoft Exchange SSRF vulnerabilities exist: CVE-2021-26855 CVE-2021-26857 CVE-2021-26858 CVE-2021-27065

Non-Compliant Rules:

Setting Name	Setting Type	Setting Description	Rule Name	Rule Description	Severity	Instance Data			
						Expression	Current Value	Instance Source	Rule Type
Setting for Exchange versions 2013, 2016, 2019	Registry Value	This setting checks the registry for the InterimUpdate value for Microsoft Exchange Versions 2013, 2016, and 2019.	InterimUpdate value must exist	This rule requires that the 'InterimUpdate' value must exist which indicates this version of Microsoft Exchange Server has not been patched.	Critical	NotEquals 0	0		Existential

This concludes how to use the CI contributed by SCCM community.

Thanks

Ram Lan

22nd Mar 2021

View update history

Uninstall updates

Recovery options

Update history

Quality Updates (50)

- 2021-03 Cumulative Update for Windows Server 2019 (1809) for x64-based Systems (KB5000822)
Successfully installed on 11-Mar-2021
- 2021-03 Cumulative Update for Windows Server 2019 for x64-based Systems (KB5000822) (3)
Last failed install attempt on 11-Mar-2021 - 0x80240034
- 2021-03 Servicing Stack Update for Windows Server 2019 for x64-based Systems (KB5000859) (3)
Last failed install attempt on 11-Mar-2021 - 0x80240034
- 2021-01 Update for Windows Server 2019 for x64-based Systems (KB4589208)
Successfully installed on 10-Mar-2021
- 2021-02 Cumulative Update Preview for Windows Server 2019 (1809) for x64-based Systems (KB4601383)
Successfully installed on 05-Mar-2021
- Security Update For Exchange Server 2019 CU8 (KB5000871)
Successfully installed on 04-Mar-2021
- Security Update For Exchange Server 2019 CU8 (KB5000871) (4)
Last failed install attempt on 04-Mar-2021 - 0x80240034
- Update for Removal of Adobe Flash Player for Windows Server 2019 for x64-based systems (KB4577586)
Successfully installed on 25-Feb-2021
- 2021-02 Cumulative Update Preview for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4602298)
Successfully installed on 25-Feb-2021
- 2021-02 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB4601887)
Successfully installed on 15-Feb-2021