Product Support Notice

PSN #	PSN028016u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.			
Original publication date: 30-Sept-24. This is Issue #2, published date: 08-Nov-24.		Severity/risk level	High	Urgency	Immediately
Name of problem	PSN028016u - VMware vCenter Server 7.0 Critical Vulnerabilities CVE-2024-38812 & CVE-2024-38813 reported on ASP 4200 R5.0				

Products affected

Avaya Solutions Platform 4200 R5.0
ASP 4200 R5.0
VMware vCenter Server 7.0

Problem description

IMPORTANT UPDATE - 11/8/2024:

Avaya has been informed by VMware by Broadcom that VCSA 7.0 U3s has not addressed **CVE-2024-38812** as stated in VMSA-2024-0019.2. VCSA 7.0 U3s fully mitigates vulnerability **CVE-2024-38813** and is still recommended for upgrade.

Avaya is working closely with VMware by Broadcom to determine if newly released VCSA 7.0 U3t fully addresses **CVE-2024-38812** as well as making sure there are no performance related issues with newer version before it can be supported and released in the next ASP 4200 R5.0 Security Service Pack.

Critical VMware vCenter Server heap-overflow and privilege escalation vulnerabilities found in vCenter 7.0 releases within the ASP 4200 R5.0 solution.

VMSA-2024-0019.2

- ~~*CVE-2024-38812:* VMware vCenter Server heap-overflow vulnerability~~
- *CVE-2024-38813:* VMware vCenter privilege escalation vulnerability

Resolution

IMPORTANT UPDATE - 11/8/2024:

Avaya has been informed by VMware by Broadcom that VCSA 7.0 U3s has not addressed **CVE-2024-38812** as stated in VMSA-2024-0019.2. VCSA 7.0 U3s fully mitigates vulnerability **CVE-2024-38813** and is still recommended for upgrade.

Only CVE-2023-38813 is mitigated in vCenter Server 7.0 U3s build 24201990. See the important updates above for more details. See the Patching section below for upgrade instructions.

Important: The N-2 direct upgrade path is not applicable to this patch PSN. The entire ASP 4200 solution must be on the latest July 2024 SSP prior to applying this PSN and upgrading to 7.0 U3s build 24201990.

July 2024 SSP: PSN028014u –Issue3- New Infrastructure Security Service Pack available for the ASP 4200 5.0 release (avaya.com)

Workaround or alternative remediation

N/A.

Remarks

11/8/2024: Issue 2 – Update to include important information communicated by our vendor on VCSA 7.0 U3s not fully addressing CVE-2024-38812. CVE-2024-38813 is still mitigated in VCSA 7.0 U3s.

09/30/2024: Issue 1 – Initial publication.

Patch Notes

Backup before applying the patch

Always.

Download

File: ASP4200_5.0_VMware-vCenter-Server-Appliance-7.0.3.02100-24201990-patch-FP.iso
PLDS ID# CPOD0000268

Patch install instructions	Service-interrupting?
	Yes

VMware vCenter Server 7.0 Update 3s build 24201990

Important: The N-2 direct upgrade path is not applicable to this patch PSN. The entire ASP 4200 solution must be on the latest July 2024 SSP prior to applying this PSN and upgrading to 7.0 U3s build 24201990.
July 2024 SSP: PSN028014u –Issue3- New Infrastructure Security Service Pack available for the ASP 4200 5.0 release (avaya.com)

For additional information reference to the vendor release notes: VMware vCenter Server 7.0 Update 3s Release Notes.
https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u3s-release-notes/index.html

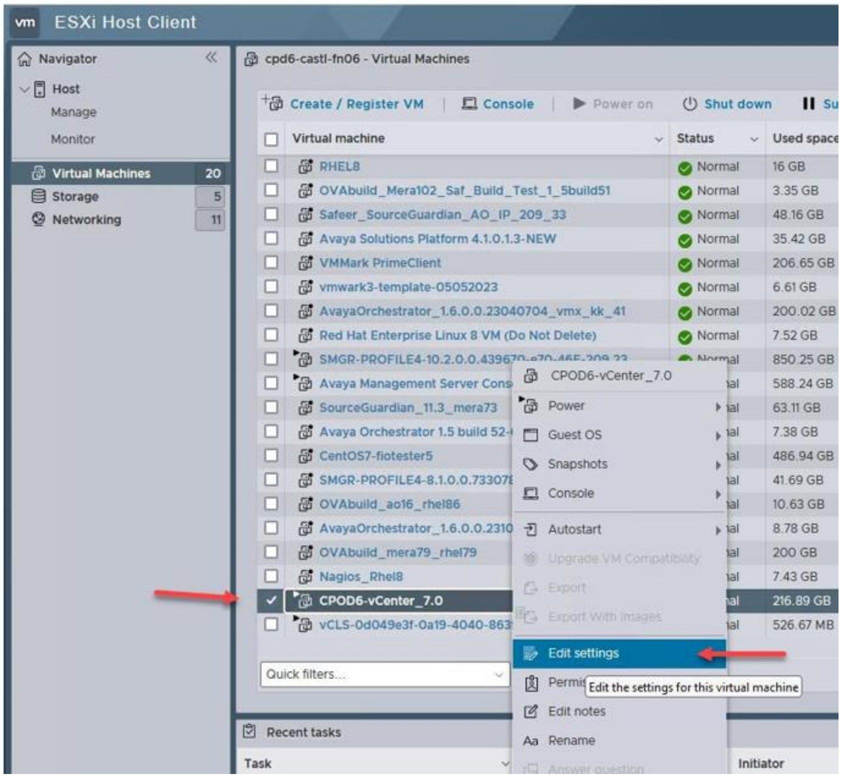
Installation instructions: Due to the observations and issues found during the upgrade, follow the procedure below to upgrade the vCenter to the new 7.0 U3s build 24201990 release.

Observations and known issues:

- When mounting the patch ISO to the vCenter Server VM CD-ROM to conduct the update, the vCenter connection gets dropped after a few minutes and is offline for up to 10 minutes. After further discussions with our vendor, anytime that a file is mounted or there is a change with the vCenter VM CD-ROM there is a question that the user must answer in order to override the lock on the CD-ROM.

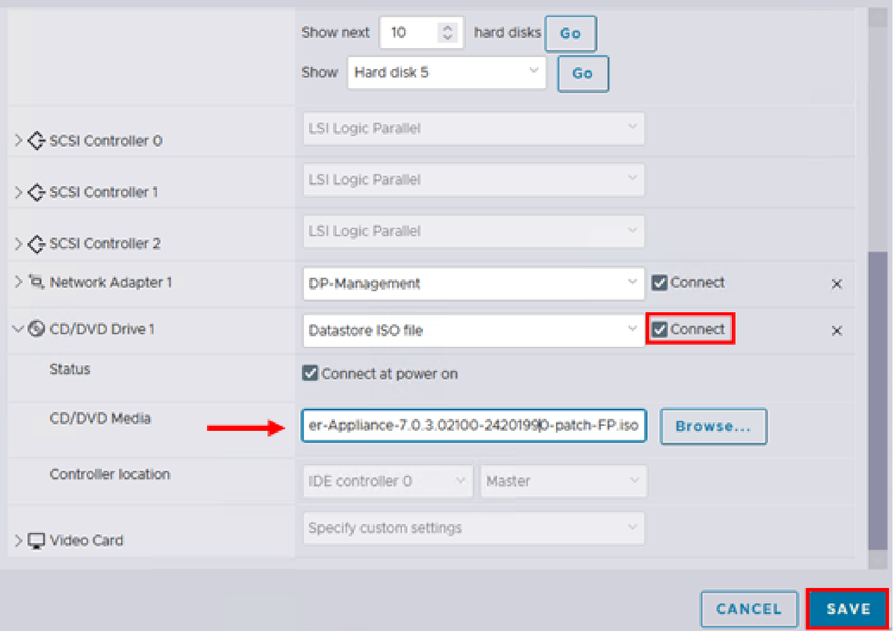
Updating the vCenter Server Appliance:

1. Connect to the MSC and log in using the Administrator account.
2. Open a web browser and enter the URL for the vSphere Web Client: https://vcenter_server_ip_address_or_fqdn/ui. Login using the administrator@vsphere.local account.
3. Click on the ⛁ icon and select storage.
4. From the menu on the left, locate and click on the Application1 datastore.
5. With the Files tab view, select the appropriate folder where the patch ISO file will be uploaded and click “upload files”.
6. Browse to the location and select the patch ISO and then select Open to begin the upload.
7. Upload process will begin. Wait until the upload is complete.
   Note: An error may occur at this step and upload may fail. Refer to the error message and note down the ESXi host IP address mentioned in the error message. Open a new browser window or tab and log into the ESXi host described in the error message (https://ESXi_host_IP) using the root credentials (refer to the Customer Lifecycle Workbook for the ESXi root account login details). After successful login, go back to step 6 and begin uploading the VCSA update file again.
8. Click on the ▯ icon to go to the Hosts and Clusters view. Locate the vCenter VM and from the summary tab take note of the ESXi host that its located on.
9. Open a new browser tab and go to the ESXi host that the vCenter VM is located. Login with the root credentials.
10. Go to Virtual Machines, select and right click the vCenter VM. Go to Edit Settings.



Virtual machine	Status	Used space
RHEL8	Normal	16 GB
OVAbuild_Mera102_Saf_Build_Test_1_5build51	Normal	3.35 GB
Safeer_SourceGuardian_AO_IP_209_33	Normal	48.16 GB
Avaya Solutions Platform 4.1.0.1.3-NEW	Normal	35.42 GB
VMMark PrimeClient	Normal	206.65 GB
vmwark3-template-05052023	Normal	6.61 GB
AvayaOrchestrator_1.6.0.0.23040704_vmx_kk_41	Normal	200.02 GB
Red Hat Enterprise Linux 8 VM (Do Not Delete)	Normal	7.52 GB
SMGR-PROFILE4-10.2.0.0.439670-e70-465-209.22	Normal	850.25 GB
Avaya Management Server Cons	ial	588.24 GB
SourceGuardian_11.3_mera73	ial	63.11 GB
Avaya Orchestrator 1.5 build 52-	ial	7.38 GB
CentOS7-fiotester5	ial	486.94 GB
SMGR-PROFILE4-8.1.0.0.73307	ial	41.69 GB
OVAbuild_ao16_rhel86	ial	10.63 GB
AvayaOrchestrator_1.6.0.0.2310	ial	8.78 GB
OVAbuild_mera79_rhel79	ial	200 GB
Nagios_Rhel8	ial	7.43 GB
☑ CPOD6-vCenter_7.0	ial	216.89 GB
vCLS-0d049e3f-0a19-4040-863	ial	526.67 MB

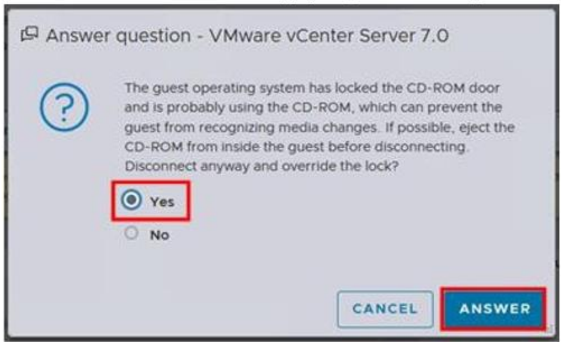
11. From the CD/DVD drive 1 option, select datastore ISO from the dropdown menu.
12. If not already, expand the CD/DVD drive 1 view and click browse.
13. Navigate to and select the VCSA update patch ISO file uploaded during step 6 and click Select to mount it to the vCenter VM CD/DVD drive.
14. Ensure that the CD/DVD drive 1 is connected and click SAVE.



Show next 10 hard disks Go
Show Hard disk 5 Go

SCSI Controller 0	LSI Logic Parallel
SCSI Controller 1	LSI Logic Parallel
SCSI Controller 2	LSI Logic Parallel
Network Adapter 1	DP-Management ☑ Connect
CD/DVD Drive 1	Datastore ISO file ☑ Connect
Status	☑ Connect at power on
CD/DVD Media	er-Appliance-7.0.3.02100-24201990-patch-FP.iso Browse...
Controller location	IDE controller 0 Master
Video Card	Specify custom settings

15. Once Save is clicked a window pops up to answer question. Select Yes and click Answer.



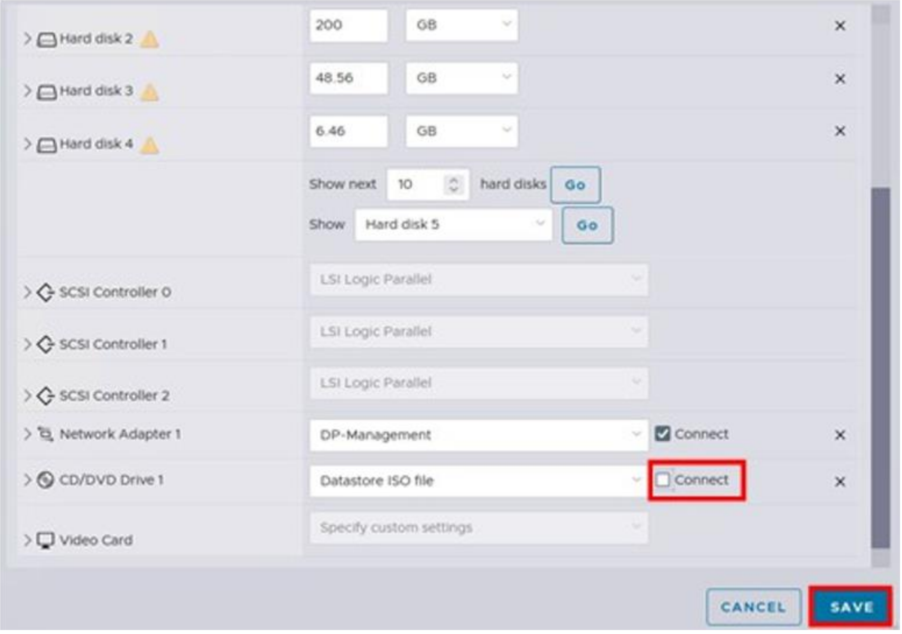
Answer question - VMware vCenter Server 7.0

The guest operating system has locked the CD-ROM door and is probably using the CD-ROM, which can prevent the guest from recognizing media changes. If possible, eject the CD-ROM from inside the guest before disconnecting. Disconnect anyway and override the lock?

● Yes

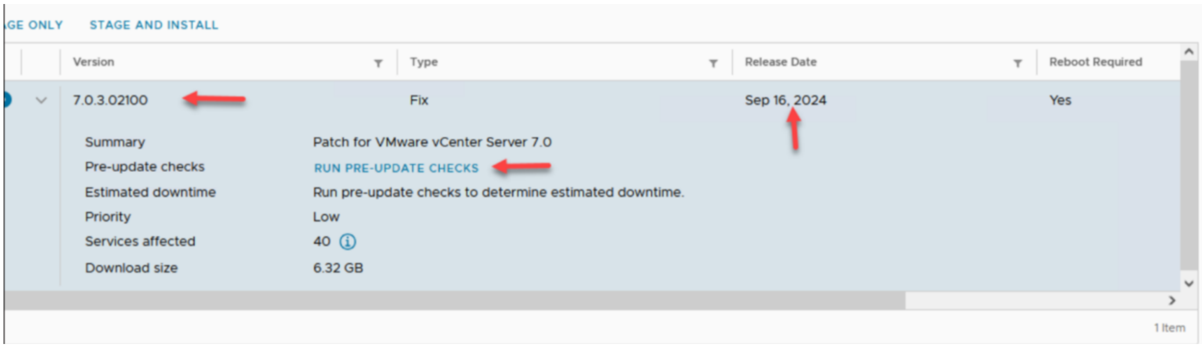
○ No

16. After answering the question, the CD/DVD drive 1 gets disconnected. Go back to Virtual Machines and select and right click the vCenter VM. Go to Edit Settings.



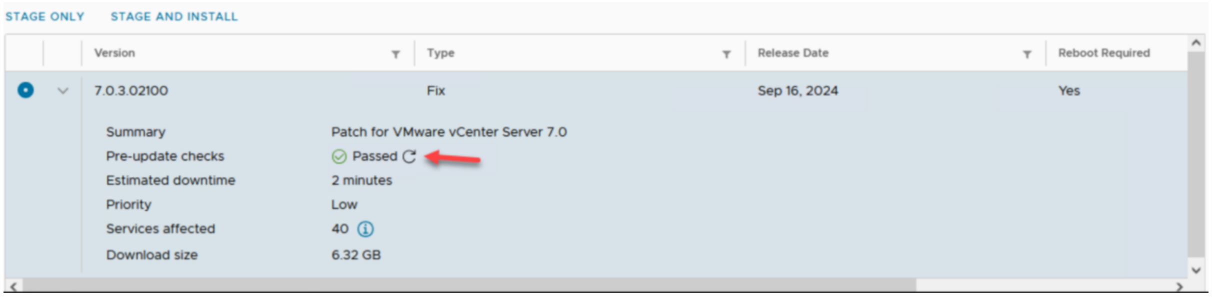
Hard disk 2	200	GB	×
Hard disk 3	48.56	GB	×
Hard disk 4	6.46	GB	×
	Show next 10 hard disks Go		
	Show Hard disk 5 Go		
SCSI Controller 0	LSI Logic Parallel		
SCSI Controller 1	LSI Logic Parallel		
SCSI Controller 2	LSI Logic Parallel		
Network Adapter 1	DP-Management	☑ Connect	×
CD/DVD Drive 1	Datastore ISO file	□ Connect	×
Video Card	Specify custom settings		

17. Check the Connect box to reconnect the CD/DVD drive 1 and click Save.
18. Open a new browser tab and go to the VCSA appliance management interface with the URL: https://vcenter_ip:5480 Log in with the root credentials.
19. Click Update in the left column.
20. Click Check Updates and select check CD ROM. The patch ISO file mounted during step 13 should now be visible under Available updates (7.0.3.02100). Click Run pre-update checks to confirm vCenter is healthy before the upgrade process begins. Pre-update checks should display passed.



Version	Type	Release Date	Reboot Required
7.0.3.02100	Fix	Sep 16, 2024	Yes

Summary	Patch for VMware vCenter Server 7.0
Pre-update checks	RUN PRE-UPDATE CHECKS
Estimated downtime	Run pre-update checks to determine estimated downtime.
Priority	Low
Services affected	40
Download size	6.32 GB



Version	Type	Release Date	Reboot Required
7.0.3.02100	Fix	Sep 16, 2024	Yes

Summary	Patch for VMware vCenter Server 7.0
Pre-update checks	Passed
Estimated downtime	2 minutes
Priority	Low
Services affected	40
Download size	6.32 GB

21. Click Stage and Install.
22. Accept the license agreement and click Next.
23. Check that a backup of the VCSA has been completed. Click Finish to start the update.
24. Once the update completes click OK.
25. If a reboot is required, go to Summary > Actions and click reboot.
26. After the reboot, log back into the vCenter Server Appliance management interface, as mentioned in step 18.
27. Click Update in the left column.
28. Verify the current VCSA version (7.0.3.02100).

Verification

See steps 26-28 above for verification.

Failure

Contact Avaya Support

Patch uninstall instructions

N/A.

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

Avaya uses the Common Vulnerability Scoring System version 3 (CVSSv3) base score and metrics as reported by the vendor for the affected component(s) or by the National Institute of Standards and Technology in the National Vulnerability Database. In some cases, such as where CVSS information is not available from the vendor or NIST, Avaya will calculate the CVSSv3 base score and metrics. Customers are encouraged to calculate the Temporal and Environmental CVSSv3 scores to determine how the vulnerability could affect their specific implementation or environment. For more information on CVSS and how the score is calculated, see Common Vulnerability Scoring.

Reference: **VMSA-2024-0019.2**

Avaya Security Vulnerability Classification

N/A

Mitigation

Reference to the patch install instructions above to mitigate the vulnerabilities.

If you require further information or assistance, please contact your Authorized Service Provider or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED "AS IS". AVAYA LLC, ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS "AVAYA"), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS' SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.