Product Support Notice

PSN #	PSN028014u			
Original publication date: 23- Jan-2024. This is Issue #08, published date: 21-March-2025.	Severity/risk level	Critical	Urgency	When Convenient

Name of problem

PSN028014u – New Infrastructure Security Service Pack available for the ASP 4200 5.0 release

Products affected

Avaya Solutions Platform 4200 5.0, ASP 4200 5.0

Problem description

New Infrastructure Security Service Pack available for the ASP 4200 5.0 release. It includes the latest software and firmware approved by Avaya Engineering for ESXi 7.0, vCenter Server 7.0, Nimble CS1000, VSP7400 network switches, PDU, PDU Router, MSC and HPE Gen9/Gen10 Servers. This Security Pack covers recently reported security vulnerabilities (CVEs) from the field as well as OEM vendor bug fixes.

The full Security Service Pack must be installed, with no individual component upgrades.

ASP4200 **4.x** racks cannot be upgraded directly to this security service pack. **Upgrade to the ASP 4200 5.0 release first** and then apply this SSP. See the supported upgrade paths table below for more details.

Resolution

See the corresponding sections below for information on each new software and firmware release and a list of vulnerabilities mitigated.

Workaround or alternative remediation

See the corresponding sections below and apply workarounds where applicable.

Remarks

IMPORTANT: The May 2024 SSP has a new PSN#. See PSN028015u for details and instructions for the May 2024 SSP release, this PSN should be used for **step-up upgrade purposes only.** See PSN028007u for details and instructions for previous 5.0 SSP releases (July 2023). Review the supported upgrade path table below for details.

Issue 8 – 03/21/2025

Issue 8 of this PSN provides an update for critical VMSA-2025-0004 vulnerability and its associated CVEs (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226). VMware ESXi 7.0 U3s patch, which mitigates the vulnerability has been tested, approved, and released by Avaya Engineering for the ASP 4200 solution. Please see **PSN028017u** for important details.

Issue 7 – 03/10/2025

Issue 7 of this PSN provides an informational update. Avaya is aware of the critical VMSA-2025-0004 vulnerability and its associated CVEs (CVE-2025-22224, CVE-2025-22225, CVE-2025-22226). We are currently assessing the new VMware ESXi 7.0 U3s patch, which mitigates the vulnerability, with support from VMware/Broadcom Engineering. This PSN will be updated as new information is available.

Issue 6 – 12/13/2024

This December 2024 update to the security service pack includes the following new SW/FW:

- vCenter Server 7.0 U3t build 24322018
- VSP 7400 VOSS v8.10.6.0
- HPE DL360 Gen10v1/v2 Server FW SPP version B7
- HPE DL360 Gen9 Server FW for System ROM (BIOS) P89 3.40
- Avaya Management Server Console (MSC) 5.0.0.0.18
- Avaya PDU router v5.0.0.0.13
- Drivers:
  - Gen10 Storage Controller: Microchip-smartpqi_70.4672.0.104-1OEM.700.1.0.15843807_24084413
  - 10GB NIC: MRVL-E3-Ethernet-iSCSI-FCoE_3.0.251.0-1OEM.700.1.0.15843807_24003260

Issue 5 – 10/11/2024

New PDU Router v5.0.0.0.12 available that mitigates several critical/high/medium level vulnerabilities. See corresponding PDU Router (Linux) section for more details.

Avaya PDU Router 5.0.0.0.12.ova – PLDS ID: **CPOD0000269**

Issue 4 – 8/27/2024

Added information for the new PSN which includes the previous May 2024 SSP details. This was added due to upgrade path changes and if a step-up upgrade is required.
HPE Nimble plugin for vCenter is unavailable/failed after upgrade to vCenter 7.0u3q or later releases. Fix is in new NimbleOS release 6.1.2.502-1057650. File has been added to the July SSP ZIP file. There is a new label for the ZIP file due to this change:
ASP4200_5.0.x_Infrastructure_Security_Service_Pack_July2024**_v2**.zip
If the July 2024 SSP has already been fully installed, the new NimbleOS SW can be downloaded from PLDS individually:
PLDS ID: **CPOD0000267**

Issue 3 – 07/04/2024

This July 2024 update to the security service pack includes the following new SW/FW:

- VMware ESXi 7.0 U3q build 23794027
- VMware vCenter Server 7.0 U3r build 24026615
- HPE Nimble OS 6.1.2.500-1053701

Issue 2 – 05/10/2024

May 2024 SSP has a new PSN#. See PSN028015u for details and instructions for the May 2024 SSP release.

This May 2024 update to the security service pack includes the following new SW/FW:

- VMware ESXi 7.0 U3p build 23307199
- Avaya EASG VIB 1.1-7
- Sentry4 PDU v80z

Issue 1 - 01/23/2024

New zip file and PLDS ID - ASP4200_5.0.x_Infrastructure_Security_Service_Pack_Jan2024.zip.
New individual PLDS IDs for the MSC and PDU Router files.

This January 2024 update to the security service pack includes the following new SW/FW:

- VMware vCenter 7.0 U3p build 22837322
- VMware ESXi 7.0 U3o build 22348816
- HPE DL360 Gen10v1/v2 Server FW SPP version B6
- HPE DL360 Gen9 Server FW SPP version B4
- HPE Nimble/Alletra version 6.1.2.300-1042680
- VSP 7400 VOSS v8.10.2.0
- Sentry4 PDU v80y
- Avaya Management Server Console (MSC) 5.0.0.0.16
- Avaya PDU router v5.0.0.0.11

Note: If there is no firmware or software listed above for a particular component (e.g., VSP 7200 switches) the latest/current version was already provided in the initial ASP 4200 5.0 release.

Procedures

The information in this section concerns the procedures, if any, recommended in the Resolution above.

Backup before conducting procedures

Yes

Download

NEW PLDS ID **CPOD0000270** – ASP4200_5.0.x_Infrastructure_Security_Service_Pack_Dec2024.zip

PLDS ID **CPOD0000259** – ASP4200_5.0.x_Infrastructure_Security_Service_Pack_July2024**_v2**.zip

PLDS ID **CPOD0000264** - ASP4200_5.0_AVA-avaya-easg_1.1-7_23348963 – (Required only for ESXi fresh installations)

Important: Due to changes in the supported upgrade path, the new zip file (created and released on 12/13/2024) does not replace the one released with the previous security service pack (May 2024, July 2024).

Upgrade FW/SW files included in the December 2024 ZIP file:

- **New** VMware-vCenter-Server-Appliance-7.0.3.02200-24322018-patch-FP.iso
- **New** bp-avaya-dl360g10-ASP4200-5-0-0-0-B7.iso
- **New** P89_3.40_08_29_2024.signed.flash
- **New** VOSS7400.8.10.6.0.tgz
- **New** MRVL-E3-Ethernet-iSCSI-FCoE_3.0.251.0-1OEM.700.1.0.15843807_24003260.zip
- **New** Microchip-smartpqi_70.4672.0.104-1OEM.700.1.0.15843807_24084413.zip
- HPE Alletra 6.1.2.502-1057650-opt.update.v2
- AVAYA-HPE-ESXi-7u3q-23794027.zip
- pro-v80z.bin
- amshelprComponent_701.11.8.5.8-1_20773446.zip

Note: If there is no firmware or software listed above for a particular component (e.g., VSP 7200 switches) the latest/current version was already provided in the initial ASP 4200 5.0 release.

Avaya Orchestrator:
IMPORTANT: A new AO 1.6 release is currently in progress at the time of the December 2024 SSP release. This PSN will be updated once the new build is available. AO 1.5 build 51 is still the current release.

- AvayaOrchestrator_1.5.0.0.23071951_vmx.ova - PLDS ID: **CPOD0000253**
- avayaorchestrator.1.5.0.051.iso - PLDS ID: **CPOD0000254**

Avaya Management Server Console (MSC):

- Avaya Management Server Console 5.0.0.0.18-esxi7.ova – PLDS ID: **CPOD0000271**

Avaya PDU Router (Linux):

- Avaya PDU Router 5.0.0.0.13.ova – PLDS ID: **CPOD0000272**

Patch Installation Instructions	Service-interrupting?
	Yes

ASP4200 **4.x** racks cannot be upgraded directly to this security service pack. **Upgrade to the ASP 4200 5.0 release first** and then apply this SSP. See the supported upgrade paths table below for more details.

Important:
After the May 2024 SSP, **Avaya will only be testing** upgrade paths from N-2 releases. For example, the only direct upgrade paths supported will be from R5.0 + **SSP Jan 2024** and **SSP May 2024** respectively. Avaya strongly recommends, as a best practice, keeping up with the infrastructure FW/BIOS and ESXi (Hypervisor) versions to prevent from having to conduct one or multiple step-up upgrades in the future.

May 2024 SSP has a new PSN#. See **PSN028015u** for details and instructions for the May 2024 SSP release.

Supported Upgrade Paths:

From ASP 4200 Release	**To ASP 4200 5.0 SSP (December 2024)**
R4.x	**Not Supported – DO NOT attempt, upgrade will fail. – See PSN028007u**
R4.1.0.1 with **11/08/2022** Security Service Pack **(Issue 14)**	**Not Supported – Have to be on the R5.0 baseline, Dec 2022 SSP, Jan 2023 SSP, or July 2023 SSP prior to upgrading. – See PSN028007u**
R5.0	**Not Supported – See PSN028015u**
R5.0 + SSP from Dec 2022	**Not Supported – See PSN028015u**
R5.0 + SSP from Jan 2023	**Not Supported – See PSN028015u**
R5.0 + SSP from July 2023	**Not Supported – See PSN028015u**
R5.0 + SSP from January 2024	**Partially Supported – Server firmware ONLY.** **See PSN028015u for upgrading the remaining components to the May 2024 SSP release prior to upgrading to the December 2024 SSP.**
R5.0 + SSP from May 2024	**Supported – No step-up upgrade required**
R5.0 + SSP from July 2024	**Supported – No step-up upgrade required**

Important:
The following software and firmware are available to be applied on ASP 4200 5.0 environments **only**. The full Security Service Pack must be installed, with **no individual component upgrades**.

Pre-requisites:

- Overall health of the infrastructure components is in a healthy state. All alarms should be resolved prior to schedule this activity.
- Identify and delete all snapshots taken for virtual machines.
- Perform a backup before beginning the upgrade process.
- The upgrade procedures should be conducted during a planned and scheduled maintenance window as they are service impacting. Please note that not all Avaya Applications support vMotion capabilities and may need to be powered down, check feature support with each application’s documentation.
- Use the workflow below when planning the maintenance activities.
- Download the corresponding ZIP file from PLDS and place it on the MSC.

Important: Avaya strongly recommends configuring SNMPv3 on all components within the ASP 4200 solution that support it to mitigate severity 4 and 5 vulnerabilities for SNMPv2.

HPE DL360 Gen9/Gen10v1/Gen10v2 Servers – Service Pack for ProLiant (SPP):
Severity/risk level: Medium / High

Gen10 v1/v2 SPP iso image:

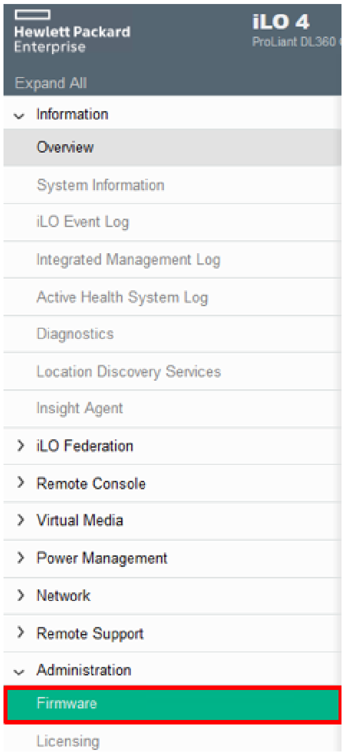
- Gen10v1/v2 SPP file: bp-avaya-dl360g10-ASP4200-5-0-0-0-B7.iso
  Installation instructions: Reference the latest MSC upgrade documentation for the procedure. https://download.avaya.com/css/public/documents/101081871

Gen9 P89 BIOS flash file:

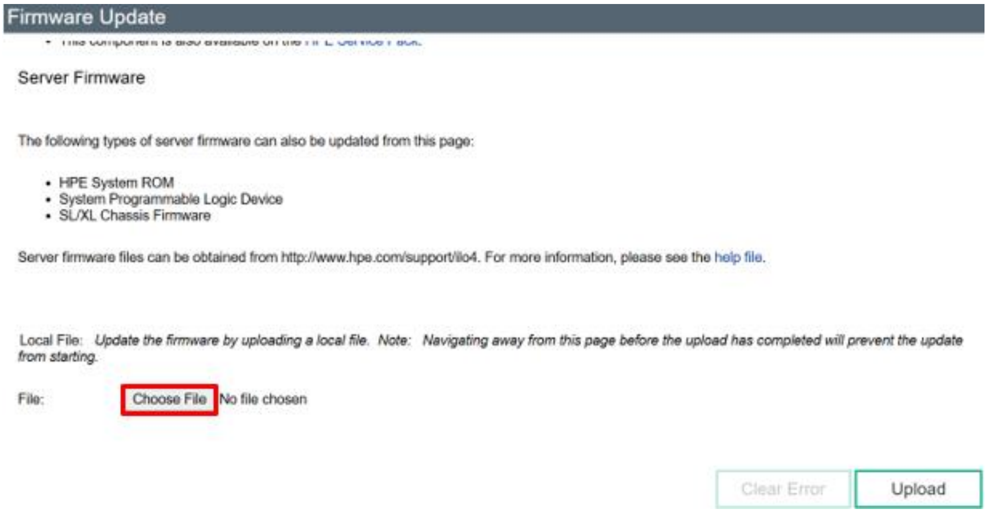
- Gen9 BIOS flash file: P89_3.40_08_29_2024.signed.flash
  Installation instructions: For the December 2024 Security Service Pack release, the only new firmware that is available for the Gen9 servers from our vendor is for the BIOS. See the instructions below to upgrade the BIOS through the iLO UI. There is no Gen9 SPP iso image for this release.

Instructions to install the Gen9 P89 v3.40 BIOS through the iLO UI:

1. Log into the vCenter Server with Administrative credentials
2. Go to the inventory, select and right click the Gen9 server and place it into maintenance mode.
3. Log into the iLO4 UI with the Administrative credentials.
4. Go to Administration > Firmware



5. Click Choose File and select the "P89_3.40_08_29_2024.signed.flash" file. Click Open.



- This component is also available on the HPE Service Pack.

Server Firmware

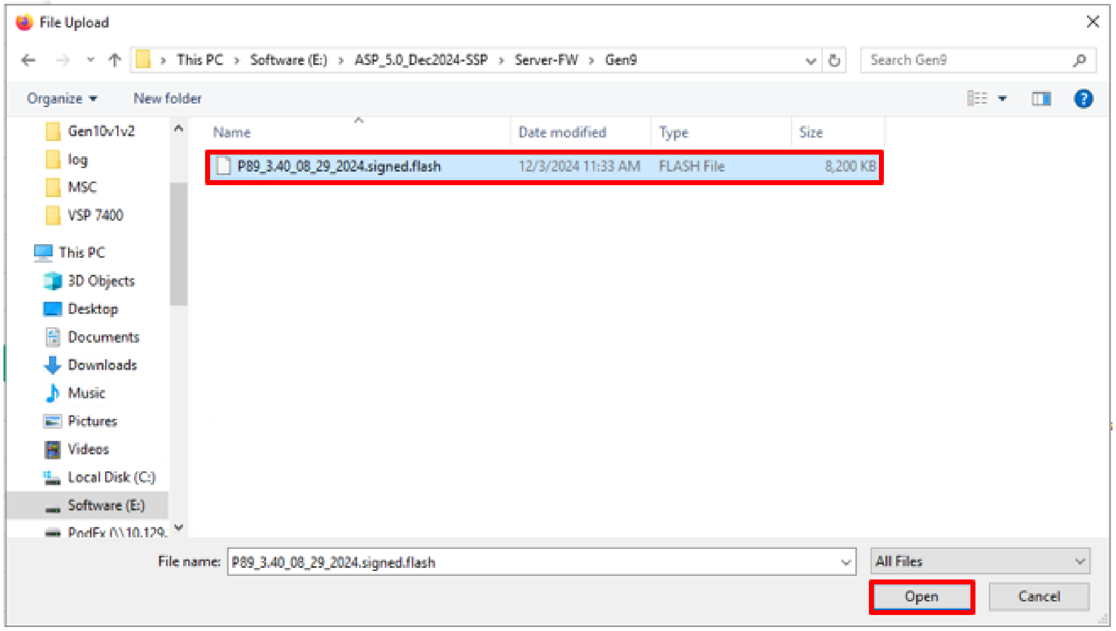
The following types of server firmware can also be updated from this page:

- HPE System ROM
- System Programmable Logic Device
- SL/XL Chassis Firmware

Server firmware files can be obtained from http://www.hpe.com/support/ilo4. For more information, please see the help file.

Local File: *Update the firmware by uploading a local file. Note: Navigating away from this page before the upload has completed will prevent the update from starting.*

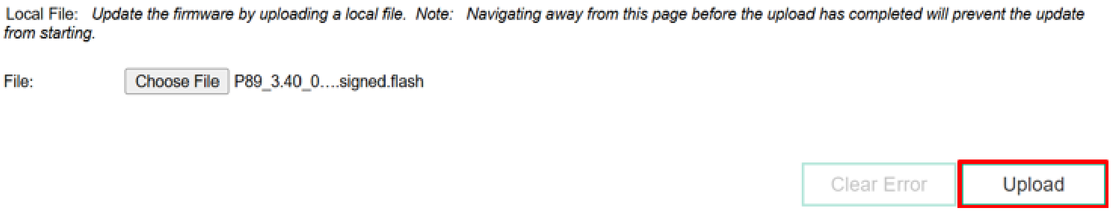
File: Choose File No file chosen



Name	Date modified	Type	Size
P89_3.40_08_29_2024.signed.flash	12/3/2024 11:33 AM	FLASH File	8,200 KB

File name: P89_3.40_08_29_2024.signed.flash

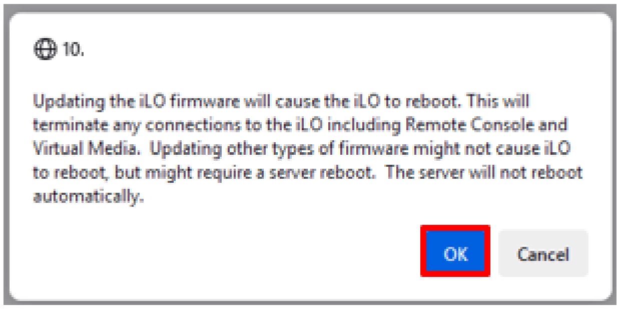
6. File is displayed. Click Upload.



Local File: *Update the firmware by uploading a local file. Note: Navigating away from this page before the upload has completed will prevent the update from starting.*

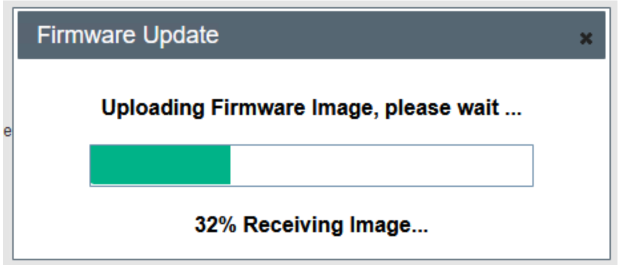
File: Choose File P89_3.40_0….signed.flash

7. Click OK.



Updating the iLO firmware will cause the iLO to reboot. This will terminate any connections to the iLO including Remote Console and Virtual Media. Updating other types of firmware might not cause iLO to reboot, but might require a server reboot. The server will not reboot automatically.

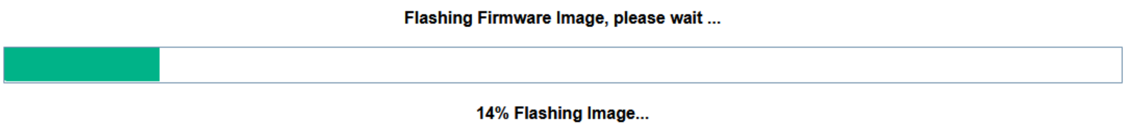
8. Uploading firmware image is displayed



Uploading Firmware Image, please wait ...

32% Receiving Image...

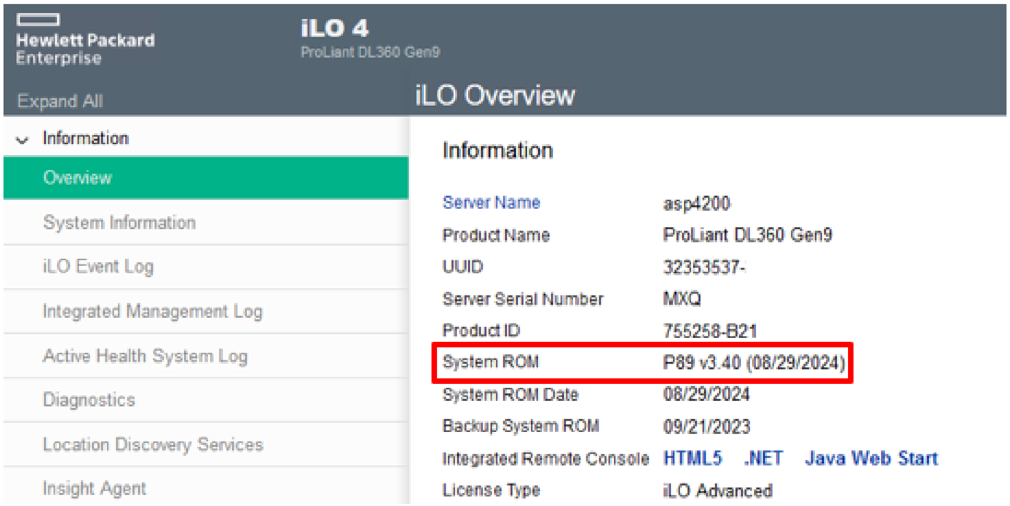
9. Displays that the firmware is flashing



Flashing Firmware Image, please wait ...

14% Flashing Image...

10. Once the firmware upgrade completes go back to the vCenter Server. Select and right click the Gen9 server and reboot it.
11. (Optional) Monitor the server boot up process by launching the HPE iLO remote console.
12. Once the Server is back online, go to the iLO4 UI and confirm that the System ROM (BIOS) displays P89 v3.40 (08/29/2024)



Information

Server Name	asp4200
Product Name	ProLiant DL360 Gen9
UUID	32353537-
Server Serial Number	MXQ
Product ID	755258-B21
System ROM	P89 v3.40 (08/29/2024)
System ROM Date	08/29/2024
Backup System ROM	09/21/2023
Integrated Remote Console	HTML5 .NET Java Web Start
License Type	iLO Advanced

13. Go back to the vCenter Server select and right click the Gen9 server and exit it from maintenance mode.
14. Repeat the procedure for the remaining Gen9 servers in the cluster.

See the observations and known issues section below for additional important information.

Contents of HPE Gen10v1/v2 SPP image (B6):

Name	Version	CVEs mitigated / Bug fixes
HPE Integrated Lights-Out 5	3.09	No vulnerabilities. Includes enhancements and bug fixes.
HPE Broadcom NX1 Firmware for 1Gb 331i NIC card	2.38 (HPE v20.30.41) BC 1.55	No vulnerabilities. Includes enhancements and bug fixes.
HPE QLogic NX2 Firmware for 10Gb 534FLR NIC card	2.35 (HPE v7.19.27) BC 7.16.15	No vulnerabilities. Includes enhancements.
HPE Smart Array P408i-p, P408e-p, P408i-a, P408i-c, E208i-p, E208e-p, E208i-c, E208i-a, P408i-sb, P408e-m, P204i-c, P204i-b, P816i-a and P416ie-m SR Gen10	7.11	No vulnerabilities. Includes enhancements and bug fixes.
HPE ProLiant DL360 Gen10 (U32) Server BIOS	3.34_2024_09_30	No vulnerabilities. Includes bug fixes.

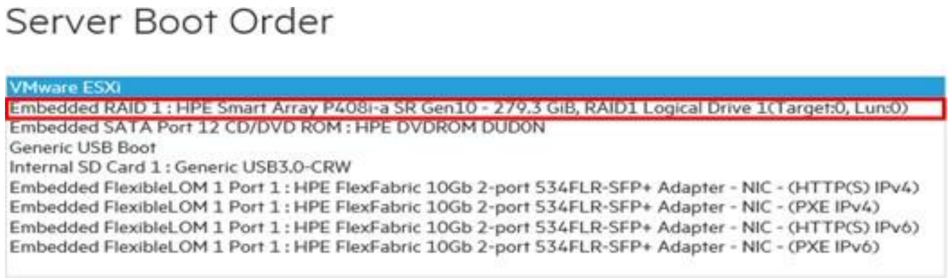
HPE Gen9 P89 BIOS flash file:

Name	Version	CVEs mitigated / Bug fixes
HPE ProLiant DL360 Gen9 (P89) Server BIOS	3.40_08_29_2024	Mitigation for CVE-2023-45229, CVE-2022-36763, CVE-2022-36764.

Observations and known issues:

- On the Gen10v1/v2 servers after the SPP firmware upgrade, the server may power off and not power back on automatically as expected. If this occurs, log into the server iLO and power it on. Once powered back on it may reboot once or twice to finish the firmware upgrades before booting into ESXi.
- On the Gen10v1/v2 servers after the SPP firmware upgrade, the boot order may get changed moving the Embedded RAID 1 Logical drive (HPE Smart Array) to the bottom of the boot order. If this occurs, then when the server reboots it will try to boot from the server's NICs first and timeouts will occur increasing server boot-up time. The server will boot from the Embedded RAID 1 controller after the NIC boot timeouts, but an increased boot-up time of 5 -10 minutes will result. This was further discussed with HPE, and this is expected behavior as designed.

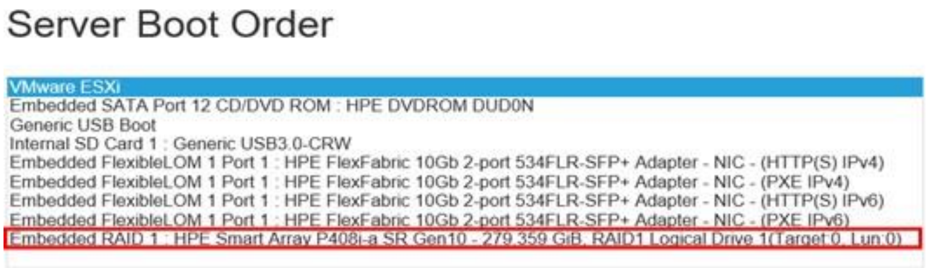
  Server boot order before firmware upgrade:
  Embedded RAID 1: HPE Smart Array is second from the top in the boot order.



Server Boot Order

```
VMware ESXi
Embedded RAID 1 : HPE Smart Array P408i-a SR Gen10 - 279.3 GiB, RAID1 Logical Drive 1(Target:0, Lun:0)
Embedded SATA Port 12 CD/DVD ROM : HPE DVDROM DUD0N
Generic USB Boot
Internal SD Card 1 : Generic USB3.0-CRW
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (HTTP(S) IPv4)
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (PXE IPv4)
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (HTTP(S) IPv6)
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (PXE IPv6)
```

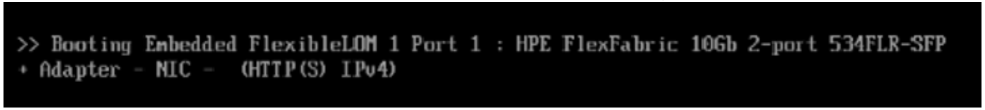
Server boot order after firmware upgrade:
Embedded RAID 1: HPE Smart Array is moved to the bottom of the boot order.



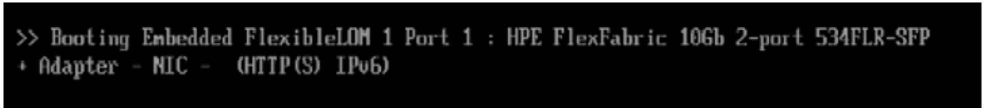
Server Boot Order

```
VMware ESXi
Embedded SATA Port 12 CD/DVD ROM : HPE DVDROM DUD0N
Generic USB Boot
Internal SD Card 1 : Generic USB3.0-CRW
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (HTTP(S) IPv4)
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (PXE IPv4)
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (HTTP(S) IPv6)
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (PXE IPv6)
Embedded RAID 1 : HPE Smart Array P408i-a SR Gen10 - 279.359 GiB, RAID1 Logical Drive 1(Target:0, Lun:0)
```

When the server reboots, it tries to boot from the NICs first before booting from the ESXi OS located on the Embedded RAID 1: HPE Smart Array :



```
>> Booting Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP
+ Adapter - NIC - (HTTP(S) IPv4)
```

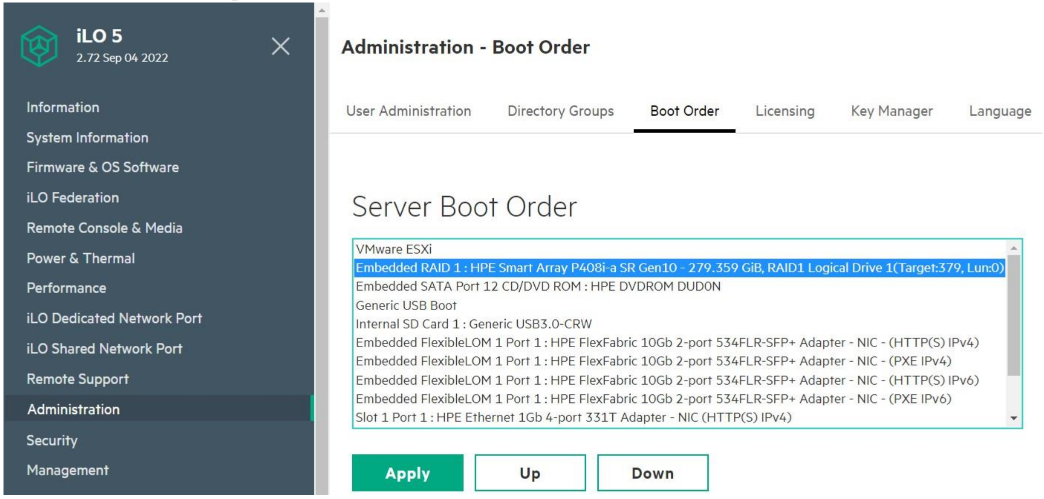


```
>> Booting Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP
+ Adapter - NIC - (HTTP(S) IPv6)
```

Note: This doesn't impact the overall ASP4200 solution, but if changes are not made, server boot-up could be delayed for 5 - 10 minutes until the server boot sequence gets to the Embedded RAID 1: HPE Smart Array.

Procedure to change the boot order back to as expected:

- Open a web browser and go to the IP or FQDN of the host iLO.
- Log in with the administrative credentials (See the customer workbook for details).
- Go to Administration > Boot Order
- Under Server Boot Order, select and highlight the Embedded RAID 1: HPE Smart ArrayP408i-a SR Gen 10 and click up until it is moved under VMware ESXi or at the top.



Administration - Boot Order

Server Boot Order

VMware ESXi
Embedded RAID 1 : HPE Smart Array P408i-a SR Gen10 - 279.359 GiB, RAID1 Logical Drive 1(Target:379, Lun:0)
Embedded SATA Port 12 CD/DVD ROM : HPE DVDROM DUD0N
Generic USB Boot
Internal SD Card 1 : Generic USB3.0-CRW
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (HTTP(S) IPv4)
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (PXE IPv4)
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (HTTP(S) IPv6)
Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP+ Adapter - NIC - (PXE IPv6)
Slot 1 Port 1 : HPE Ethernet 1Gb 4-port 331T Adapter - NIC (HTTP(S) IPv4)

- Click Apply to save the changes.

VMware:

Severity/risk level: Critical / High

VMware vCenter Server 7.0 Update 3t build 24322018

CVEs/Vulnerabilities mitigated: **CVE-2024-38812**. Includes bug fixes as well as fixes for previous known issues and vulnerabilities.

For additional information reference to the vendor release notes: VMware vCenter Server 7.0 Update 3t Release Notes

If a catastrophic failure occurs and a fresh install is required, the ISO image can be downloaded from PLDS. Do not use this ISO image for updates/upgrades. PLDS ID: **CPOD0000273** - File: **VMware-VCSA-all-7.0.3-24322018.iso**

Installation instructions: Reference the latest MSC upgrade documentation for the procedure. https://download.avaya.com/css/public/documents/101081871

Observations and known issues:

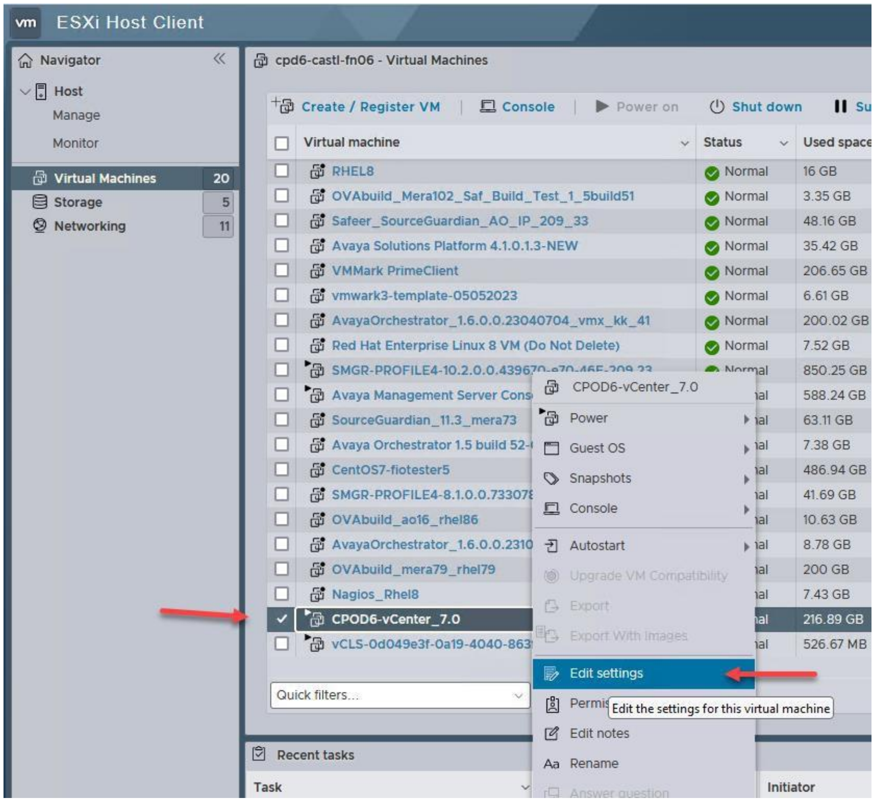
- ➢ When mounting the patch ISO to the vCenter Server VM CD-ROM to conduct the update, the vCenter connection gets dropped after a few minutes and is offline for up to 10 minutes. After further discussions with our vendor, anytime that a file is mounted or there is a change with the vCenter VM CD-ROM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

Note: This is seen when mounting the patch upgrade ISO in vCenter builds released in Jan 2023 SSP and newer.

Updating the vCenter Server Appliance:

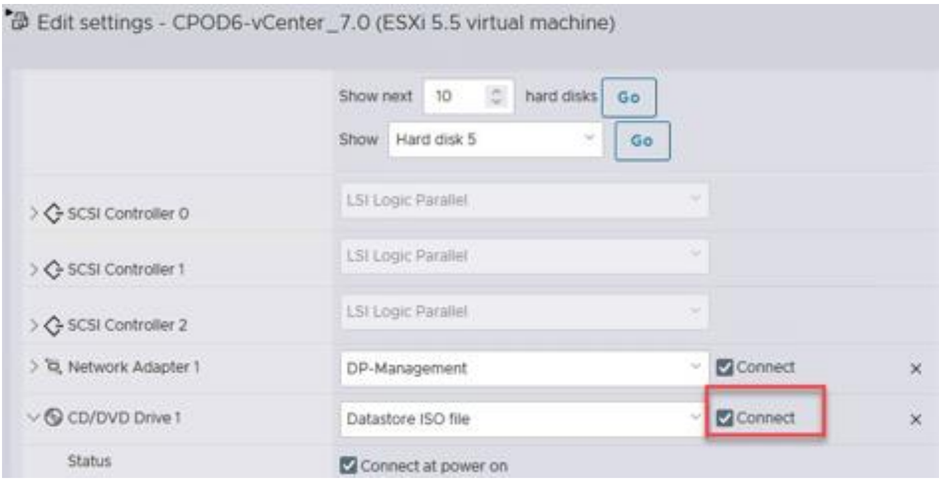
1. Connect to the MSC and log in using the Administrator account.
2. Open a web browser and enter the URL for the vSphere Web Client: https://vcenter_server_ip_address_or_fqdn/ui. Login using the administrator@vsphere.local account.
3. Click on the icon and select storage.
4. From the menu on the left, 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-e70-46E-209 23	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 OK.



Edit settings - CPOD6-vCenter_7.0 (ESXi 5.5 virtual machine)

Show next 10 hard disks
Show Hard disk 5

SCSI Controller 0: LSI Logic Parallel

SCSI Controller 1: LSI Logic Parallel

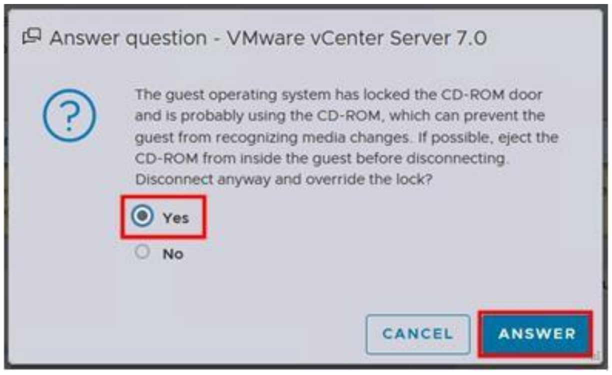
SCSI Controller 2: LSI Logic Parallel

Network Adapter 1: DP-Management ☑ Connect

CD/DVD Drive 1: Datastore ISO file ☑ Connect

Status: ☑ Connect at power on

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

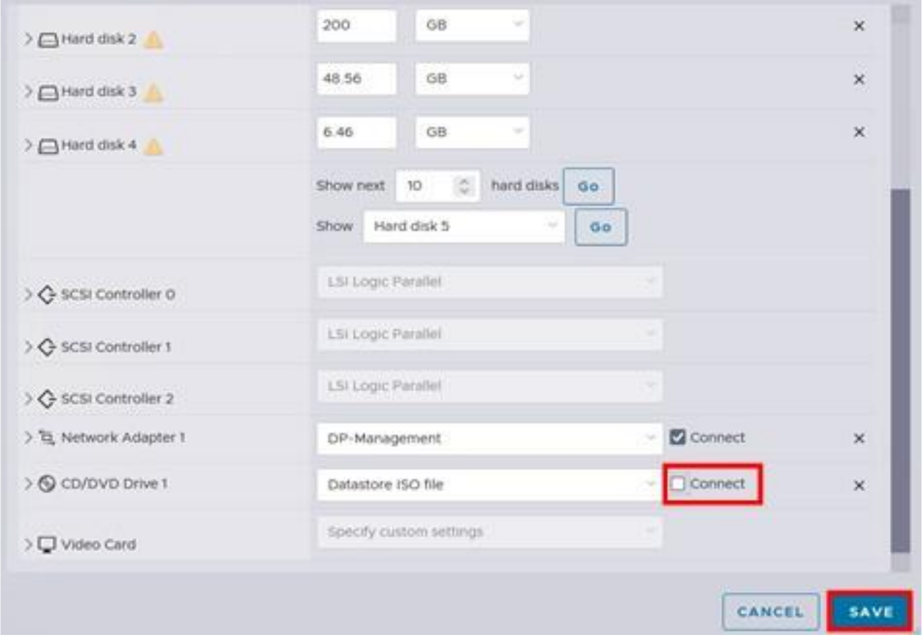


Answer question - VMware vCenter Server 7.0

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.
17. Check the *Connect* box to reconnect the CD/DVD drive 1 and click Save.



Hard disk 2: 200 GB

Hard disk 3: 48.56 GB

Hard disk 4: 6.46 GB

Show next 10 hard disks
Show Hard disk 5

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

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 (7.0.3.02200).

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 (7.0.3.02200).

VMware/HPE ESXi 7.0 Update 3q build 23794027 (Avaya customized)

March 21st, 2025 update: VMware ESXi 7.0 U3s patch, which mitigates the VMSA-2025-0004 vulnerability has been tested, approved, and released by Avaya Engineering for the ASP 4200 solution. Please see **PSN028017u** for important details.

This ESXi release is customized by Avaya to include ESXi 7.0 U3q build 23794027 with updated HPE addon version 703.0.0.11.6.0.5 and Avaya EASG 1.1-7 vib.

Note: Avaya EASG 1.1-7 vib (released with May 2024 SSP) fixes a labeling issue introduced by vCenter when adding hosts to a cluster where the local vmfs volume “datastore1” gets renamed to “datastore1 (1), (2), (3)…etc” as hosts are being added to the exiting ASP4200 cluster which introduces special characters that were not supported by the previous EASG vib. When conducting updates to the May 2024 SSP or installing the new EASG vib to a freshly deployed ESXi host, the user is no longer required, as a prerequisite, to rename the local datastore as instructed in the latest Management Server Console upgrade document.

VMSA-2024-0011 & VMSA-2024-0013

CVEs/Vulnerabilities mitigated: **CVE-2024-37086, CVE-2024-22273**. Includes bug fixes as well as fixes for previous known issues and vulnerabilities.

For additional information reference to the vendor release notes: https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-esxi-70u3q-release-notes/index.html

Important: VMware ESXi 7.0 U3c build 19193900 upgrade ISO file from initial Release 5.0 or ESXi 7.0 builds from the previous 5.0 SSP’s **must be** installed before upgrading to the ESXi 7.0 U3q patch release, no direct upgrade from N-3 and older releases. See the supported upgrade paths table above for more details.

vSphere Quick Boot

Important: Avaya strongly recommends enabling quick boot when remediating ESXi hosts as this significantly reduces the server down time.

vSphere Quick Boot is an innovation in conjunction with major server vendors that restarts the VMware ESXi™ hypervisor without rebooting the physical compute server. A regular reboot involves a full power cycle that requires firmware and device initialization. If it takes several minutes, or more, for the physical hardware to initialize devices and perform necessary self-tests, then that is the approximate time savings to expect when using the Quick Boot feature. This time saving is per Host, therefore in racks with multiple servers this will considerably reduce the compute server down time and overall maintenance activity.

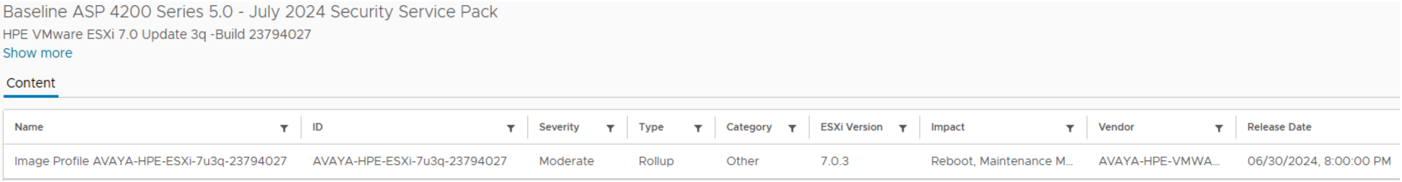
Note: The HPE Compute servers supported in the ASP 4200 R5.0 baseline support the vSphere quick boot feature.

vSphere Lifecycle Manager (vLCM) information

Image profile name/ID:

AVAYA-HPE-ESXi-7u3q-23794027 /

AVAYA-HPE-ESXi-7u3q-23794027

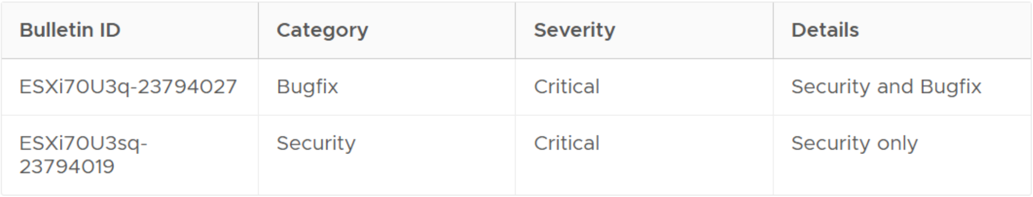


Baseline ASP 4200 Series 5.0 - July 2024 Security Service Pack

HPE VMware ESXi 7.0 Update 3q -Build 23794027

Name	ID	Severity	Type	Category	ESXi Version	Impact	Vendor	Release Date
Image Profile AVAYA-HPE-ESXi-7u3q-23794027	AVAYA-HPE-ESXi-7u3q-23794027	Moderate	Rollup	Other	7.0.3	Reboot, Maintenance M...	AVAYA-HPE-VMWA...	06/30/2024, 8:00:00 PM

Rollup Bulletin



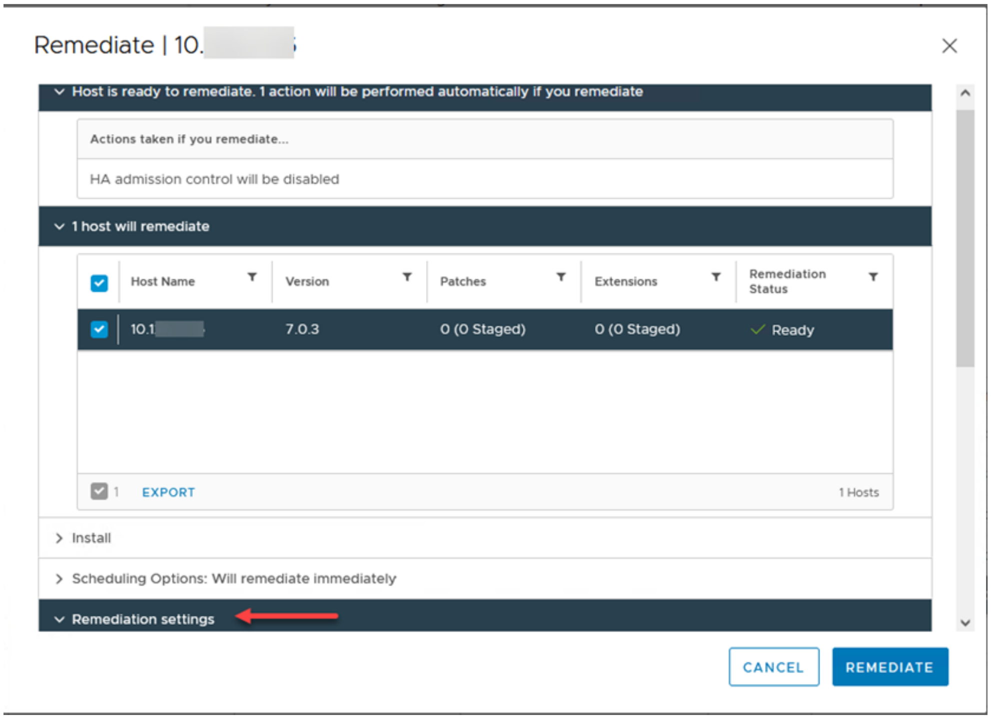
Bulletin ID	Category	Severity	Details
ESXi70U3q-23794027	Bugfix	Critical	Security and Bugfix
ESXi70U3sq-23794019	Security	Critical	Security only

Installation instructions: Reference the latest MSC upgrade documentation for the procedure. https://download.avaya.com/css/public/documents/101081871

Enabling Quick Boot in vLCM

Important: Avaya strongly recommends enabling quick boot when remediating ESXi hosts as this significantly reduces the server down time.

- In the ***Remediate*** page, click to expand ***Remediation settings.***



Remediate | 10.[redacted]

Host is ready to remediate. 1 action will be performed automatically if you remediate

Actions taken if you remediate...

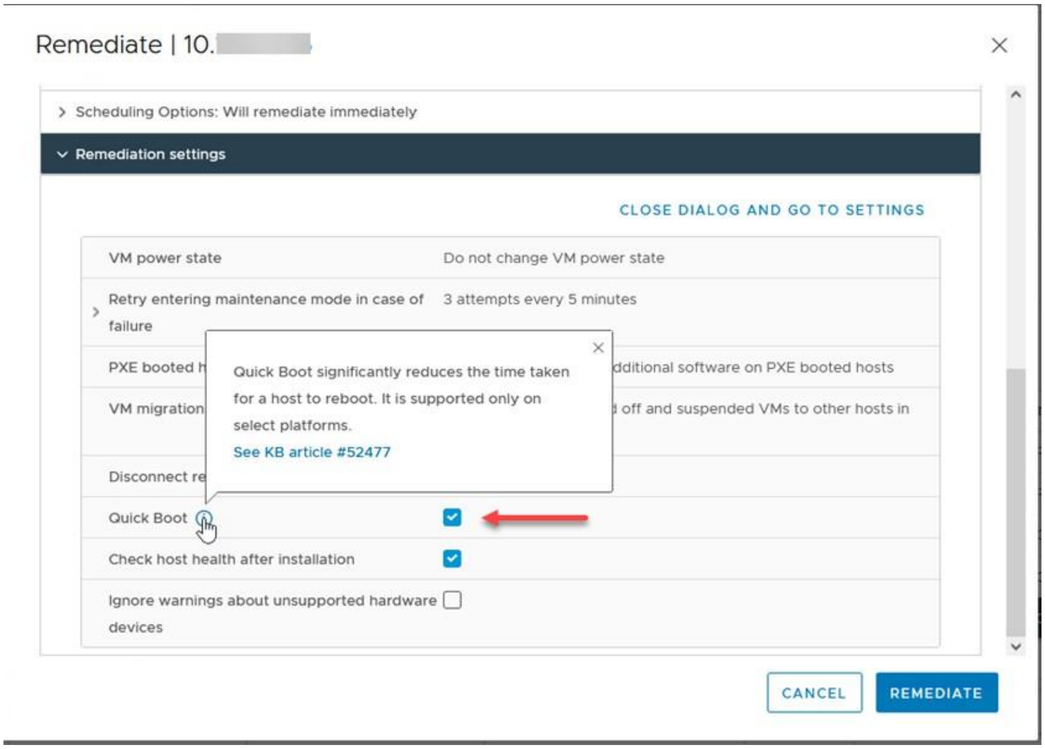
HA admission control will be disabled

1 host will remediate

☑	Host Name	Version	Patches	Extensions	Remediation Status
☑	10.1[redacted]	7.0.3	0 (0 Staged)	0 (0 Staged)	✓ Ready

Scheduling Options: Will remediate immediately

- Select the check box for ***Quick Boot***


Remediate | 10.[redacted]

Scheduling Options: Will remediate immediately

Remediation settings

VM power state	Do not change VM power state
Retry entering maintenance mode in case of failure	3 attempts every 5 minutes
PXE booted h	dditional software on PXE booted hosts
VM migration	d off and suspended VMs to other hosts in
Disconnect re	
Quick Boot	☑
Check host health after installation	☑
Ignore warnings about unsupported hardware devices	□

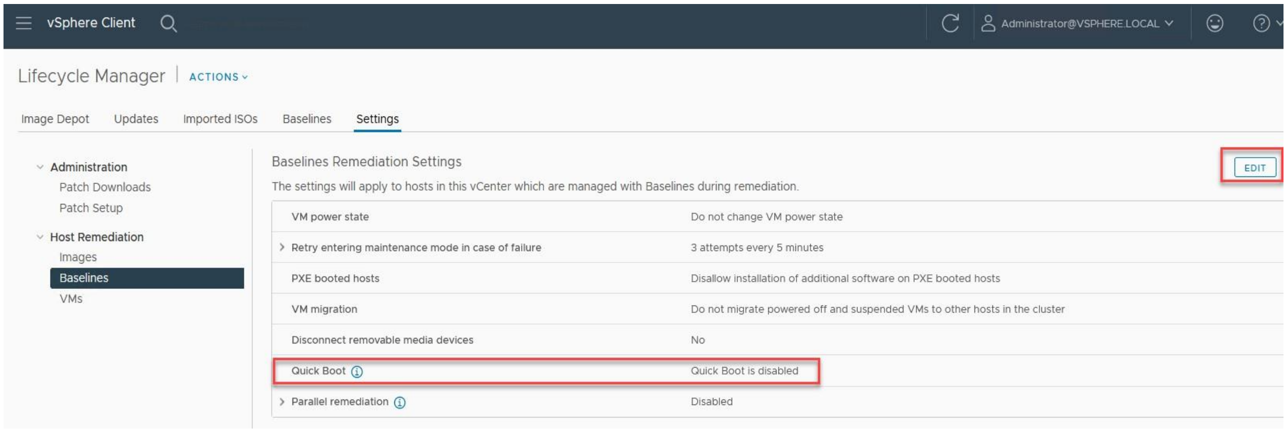
Quick Boot significantly reduces the time taken for a host to reboot. It is supported only on select platforms.
See KB article #52477

- ➢ Proceed with the remediation process as instructed in the latest MSC upgrade document https://download.avaya.com/css/public/documents/101081871

<u>Note:</u> Quick boot is disabled by default, and it must be enabled <u>every time</u> a host or cluster remediation is conducted. Alternatively, this feature can be enabled at the Lifecycle Manager-Baseline Remediation level.

<u>Follow below steps no enable quick boot globally:</u>

- ➢ At the top-left of the window, click the three lines. From the drop-down menu, select *Lifecycle Manager*.
- ➢ Navigate to *Settings* ➔ *Host Remediation* ➔ *Baseline.*
- ➢ Click the *EDIT* button.



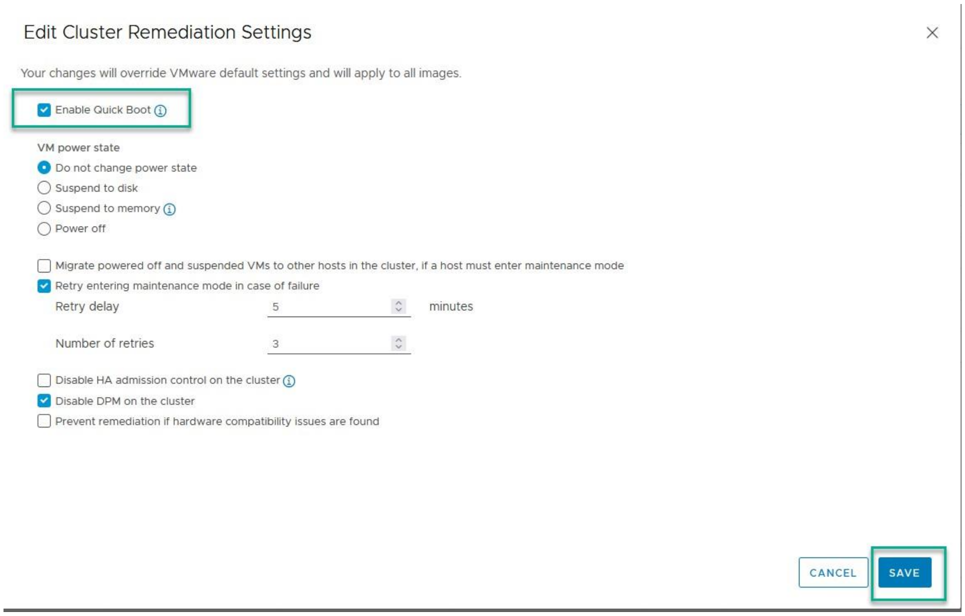
Baselines Remediation Settings

The settings will apply to hosts in this vCenter which are managed with Baselines during remediation.

VM power state	Do not change VM power state
Retry entering maintenance mode in case of failure	3 attempts every 5 minutes
PXE booted hosts	Disallow installation of additional software on PXE booted hosts
VM migration	Do not migrate powered off and suspended VMs to other hosts in the cluster
Disconnect removable media devices	No
Quick Boot	Quick Boot is disabled
Parallel remediation	Disabled

- ➢ Select the checkbox to enable ***Quick Boot.***

- Click *SAVE.*



Edit Cluster Remediation Settings

Your changes will override VMware default settings and will apply to all images.

☑ Enable Quick Boot

VM power state

● Do not change power state
○ Suspend to disk
○ Suspend to memory
○ Power off

□ Migrate powered off and suspended VMs to other hosts in the cluster, if a host must enter maintenance mode
☑ Retry entering maintenance mode in case of failure

Retry delay 5 minutes

Number of retries 3

□ Disable HA admission control on the cluster
☑ Disable DPM on the cluster
□ Prevent remediation if hardware compatibility issues are found

Qlogic, AMS, and Storage Controller Drivers:

Severity/risk level: Low

QLogic 10Gb qfle3 driver update version 1.4.51.0

IMPORTANT: This driver is only supported on the Gen10v1/v2 servers. It is not supported on the Gen9 servers. Creating separate driver baselines in vLCM will be required for the Gen9 and Gen10 servers.

STOP! - IMPORTANT: Before beginning the qfle3 driver update to the latest version 1.4.51.0, **confirm that the unused qfle3i, qfle3f, and qcnic drivers are not enabled on the host**.

Important: After an ESXi host upgrade and/or Qlogic driver update, confirm that the FCoE and the unused qfle3i, qfle3f, and qcnic drivers stay disabled on the host.

Installation instructions: Reference the latest MSC upgrade documentation for the procedure. https://downloads.avaya.com/css/P8/documents/101070494, https://download.avaya.com/css/public/documents/101081871

For Gen10v1/v2 servers - After both firmware and driver updates, the following should be observed when running the network commands on vmnics:

MFW/Firmware: ***7.16.15***

Driver Version: ***1.4.51.0***

For Gen9 servers - The following should be observed when running the network commands on vmnics:

IMPORTANT: Due to firmware compatibility with the HPE DL360 Gen9 servers, firmware 7.16.5 installed with the B4 ISO is the latest and the last supported firmware for the 10Gb NIC on the Gen9 servers. Driver version 1.4.46.0 was automatically installed with ESXi 7.0 U3q in the July SSP.

MFW/Firmware: ***7.16.5***
Driver Version: ***1.4.46.0***

Agentless Management Service (AMS)
Gen9 AMS version **11.8.5.8-1** (Latest since Dec 2022 SSP - also included in Dec 2024 SSP)
Gen10 AMS version **11.10.0.4-1** (Installed via the July 2024 ESXi 7.0 U3q patch)
Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://downloads.avaya.com/css/P8/documents/101070494, https://download.avaya.com/css/public/documents/101081871

Storage Controller
Gen9 Storage Controller version **70.0051.0.100** (Was installed via the Jan 2024 ESXi patch)
Gen10 Storage Controller version **70.4672.0.104**
Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://downloads.avaya.com/css/P8/documents/101070494,
https://download.avaya.com/css/public/documents/101081871

Avaya Orchestrator 1.5

Severity/risk level: High/Critical

This new AO 1.5 build 51 includes security fixes to multiple vulnerabilities identified on previous AO versions up to **July 1st, 2023**. Any newer vulnerabilities identified after cutover date will be addressed in the next release.

CVEs/Vulnerabilities mitigated:
QID: 241589 - Red Hat Update for emacs (RHSA-2023:3481)
CVE Number = CVE-2022-48339

QID: 241522 - Red Hat Update for apr-util (RHSA-2023:3145)
CVE Number = CVE-2022-25147

QID: 241402 - Red Hat Update for libwebp (RHSA-2023:2077)
CVE Number = CVE-2023-1999

QID: 241313 - Red Hat Update for httpd (RHSA-2023:1593)
CVE Number = CVE-2023-25690

QID: 241274 - Red Hat Update for Open Secure Sockets Layer (OpenSSL) (RHSA-2023:1335)
CVE Number = CVE-2023-0286

QID: 241271 - Red Hat Update for nss (RHSA-2023:1332)
CVE Number = CVE-2023-0767

QID: 241242 - Red Hat Update for zlib (RHSA-2023:1095)
CVE Number = CVE-2022-37434

QID: 241393 - Red Hat Update for kernel (RHSA-2023:1987)
CVE Number = CVE-2022-43750

QID: 241249 - Red Hat Update for kernel (RHSA-2023:1091)

CVE Number = CVE-2022-4378, CVE-2022-42703

QID:86445 - Web Directories Listable Vulnerability (tcp)

CVE Number = None

Reference to the latest AO release notes for the list of vulnerabilities mitigated and bug fixes in build 51. https://download.avaya.com/css/public/documents/101082027

Installation instructions: Reference to the latest *Configuring and Administering Avaya Orchestrator* documentation for upgrades, updates, and fresh installs of AO. https://downloads.avaya.com/css/P8/documents/101061680

VSP Switches:

Severity/risk level: Low

VSP7400 network switches VOSS 8.10.6.0
For upgrade instructions, reference PSN028006u.

Validated upgrade path:

- 8.9.x to 8.10.x
- 8.8.x to 8.10.x

Warning:
VOSS FW 8.10.x is not supported on the VSP 7200 switches with the ASP4200 Solution. **DO NOT** attempt to upgrade the VSP 7200 switches to VOSS 8.10.x as **this is not supported**.

CVEs/Vulnerabilities mitigated: N/A
Includes bug fixes and incorporates all fixes from prior releases, for complete list reference to:
VSP Operating System Software - Customer Release Notes for VOSS Version 8.10.6.0

PDUs:

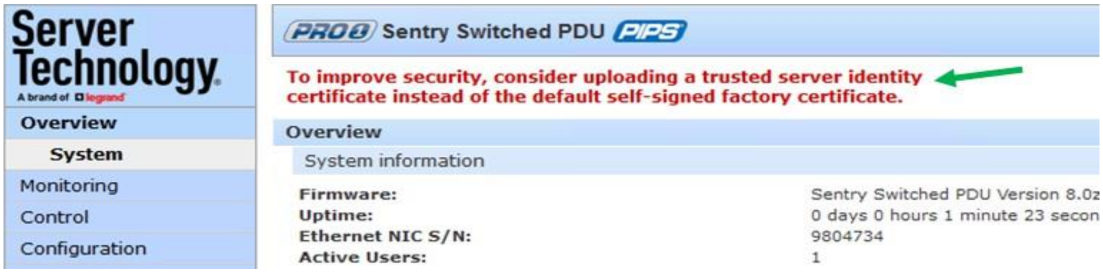
Severity/risk level: High/Critical

Sentry4 PDU version v80z
CVEs/Vulnerabilities mitigated: Additional fixes for critical CVE-2020-11901. This is a new-feature, maintenance and security patch release.
Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://download.avaya.com/css/public/documents/101081871

Observations:

- After upgrading the Sentry4 PDU to version v80z, a message is displayed in the UI recommending user to install a CA-signed certificate instead of using the self-signed certificate.

Note: Avaya strongly recommends replacing self-signed certificates with CA signed certificates in production environments.



To improve security, consider uploading a trusted server identity certificate instead of the default self-signed factory certificate.

Overview

System information

Firmware: Sentry Switched PDU Version 8.0z
Uptime: 0 days 0 hours 1 minute 23 secon
Ethernet NIC S/N: 9804734
Active Users: 1

Avaya Management Server Console (MSC):

Severity/risk level: **High/Critical**

Avaya Management Server Console 5.0.0.0.18

This new MSC build 5.0.0.0.18 includes security fixes to multiple vulnerabilities identified on previous MSC versions up to **November 21st, 2024**. Any newer vulnerabilities identified after cutover date will be addressed in the next release.

Vulnerabilities mitigated:

QID: 92111 - Microsoft Windows Security Update for February 2024
CVE-2024-21342, CVE-2024-21377, CVE-2024-21420, CVE-2024-21412, CVE-2024-21406, CVE-2024-21405, CVE-2024-21391, CVE-2024-21375, CVE-2024-21372, CVE-2024-21371, CVE-2024-21370, CVE-2024-21369, CVE-2024-21368, CVE-2024-21367, CVE-2024-21366, CVE-2024-21365, CVE-2024-21363, CVE-2024-21362, CVE-2024-21361, CVE-2024-21360, CVE-2024-21359, CVE-2024-21358, CVE-2024-21357, CVE-2024-21356, CVE-2024-21355, CVE-2024-21354, CVE-2024-21352, CVE-2024-21351, CVE-2024-21350, CVE-2024-21349, CVE-2024-21348, CVE-2024-21347, CVE-2024-21346, CVE-2024-21344, CVE-2024-21343, CVE-2024-21341, CVE-2024-21340, CVE-2024-21339, CVE-2024-21338, CVE-2024-21304, CVE-2024-20684, CVE-2024-21315.

QID: 92128 - Microsoft Windows Security Update for April 2024
CVE-2024-26180, CVE-2024-20678, CVE-2024-20669, CVE-2024-29064, CVE-2024-29062, CVE-2024-20665, CVE-2024-23594, CVE-2024-23593, CVE-2024-29050, CVE-2024-26229, CVE-2024-28901, CVE-2024-28923, CVE-2024-26240, CVE-2024-26216, CVE-2024-26241, CVE-2024-26218, CVE-2024-26194, CVE-2024-26217, CVE-2024-26214, CVE-2024-26172, CVE-2024-26254, CVE-2024-29052, CVE-2024-26253, CVE-2024-26252, CVE-2024-26230, CVE-2024-26212, CVE-2024-26244, CVE-2024-26213, CVE-2024-29061, CVE-2024-28907, CVE-2024-26226, CVE-2024-26220, CVE-2024-28903, CVE-2024-29066, CVE-2024-29056, CVE-2024-26239, CVE-2024-26211, CVE-2024-26232, CVE-2024-26243, CVE-2024-21447, CVE-2024-26245, CVE-2024-29988, CVE-2024-28898, CVE-2024-26236, CVE-2024-28904, CVE-2024-28902, CVE-2024-20688, CVE-2024-28905, CVE-2024-28900, CVE-2024-28897, CVE-2024-28896, CVE-2024-28925, CVE-2024-28924, CVE-2024-28919, CVE-2024-28921, CVE-2024-28922, CVE-2024-28920, CVE-2024-26228, CVE-2024-26215, CVE-2024-26208, CVE-2024-26207, CVE-2024-26242, CVE-2024-26237, CVE-2024-26235, CVE-2024-26234, CVE-2024-26210, CVE-2024-26158, CVE-2024-26205, CVE-2024-26200, CVE-2024-26179, CVE-2024-26256, CVE-2024-26255, CVE-2024-26250, CVE-2024-26248, CVE-2024-26219, CVE-2024-26209, CVE-2024-26202, CVE-2024-26195, CVE-2024-26189, CVE-2024-26183, CVE-2024-26175, CVE-2024-26171, CVE-2024-26168, CVE-2024-20693, CVE-2024-20689.

QID: 92131 - Microsoft Windows Domain Name System (DNS) Server Remote Code Execution (RCE) Vulnerability for April 2024
CVE-2024-26233, CVE-2024-26231, CVE-2024-26227, CVE-2024-26224, CVE-2024-26223, CVE-2024-26222, CVE-2024-26221

QID: 92149 - Microsoft Windows Security Update for July 2024
CVE-2024-39684, CVE-2024-38517, CVE-2024-38112, CVE-2024-38105, CVE-2024-38104,

CVE-2024-38102, CVE-2024-38101, CVE-2024-38100, CVE-2024-38099, CVE-2024-38091, CVE-2024-38085, CVE-2024-38080, CVE-2024-38079, CVE-2024-38078, CVE-2024-38077, CVE-2024-38076, CVE-2024-38074, CVE-2024-38073, CVE-2024-38072, CVE-2024-38071, CVE-2024-38070, CVE-2024-38069, CVE-2024-38068, CVE-2024-38067, CVE-2024-38066, CVE-2024-38065, CVE-2024-38064, CVE-2024-38062, CVE-2024-38061, CVE-2024-38060, CVE-2024-38059, CVE-2024-38058, CVE-2024-38057, CVE-2024-38056, CVE-2024-38055, CVE-2024-38054, CVE-2024-38053, CVE-2024-38052, CVE-2024-38051, CVE-2024-38050, CVE-2024-38049, CVE-2024-38048, CVE-2024-38047, CVE-2024-38044, CVE-2024-38043, CVE-2024-38041, CVE-2024-38034, CVE-2024-38033, CVE-2024-38032, CVE-2024-38031, CVE-2024-38030, CVE-2024-38028, CVE-2024-38027, CVE-2024-38025, CVE-2024-38022, CVE-2024-38019, CVE-2024-38017, CVE-2024-38015, CVE-2024-38013, CVE-2024-38011, CVE-2024-38010, CVE-2024-37989, CVE-2024-37988, CVE-2024-37987, CVE-2024-37986, CVE-2024-37985, CVE-2024-37984, CVE-2024-37981, CVE-2024-37978, CVE-2024-37977, CVE-2024-37975, CVE-2024-37974, CVE-2024-37973, CVE-2024-37972, CVE-2024-37971, CVE-2024-37970, CVE-2024-37969, CVE-2024-3596, CVE-2024-35270, CVE-2024-30098, CVE-2024-30081, CVE-2024-30079, CVE-2024-30071, CVE-2024-30013, CVE-2024-28899, CVE-2024-26184, CVE-2024-21417, CVE-2024-38186, CVE-2024-38187, CVE-2024-38185, CVE-2024-38165, CVE-2024-38191, CVE-2024-38184, CVE-2024-38161.

QID: 92160 - Microsoft Windows Security Update for August 2024
CVE-2024-38155, CVE-2024-38152, CVE-2024-38146, CVE-2024-38143, CVE-2024-38140, CVE-2024-38134, CVE-2024-38127, CVE-2024-38122, CVE-2024-38117, CVE-2024-38114, CVE-2024-38106, CVE-2024-38193, CVE-2024-38178, CVE-2024-38223, CVE-2024-38215, CVE-2024-38214, CVE-2024-38120, CVE-2022-3775, CVE-2024-38180, CVE-2024-38154, CVE-2024-38153, CVE-2024-38151, CVE-2024-38150, CVE-2024-38148, CVE-2024-38147, CVE-2024-38145, CVE-2024-38144, CVE-2024-38142, CVE-2024-38141, CVE-2024-38138, CVE-2024-38137, CVE-2024-38136, CVE-2024-38135, CVE-2024-38133, CVE-2024-38132, CVE-2024-38131, CVE-2024-38130, CVE-2024-38128, CVE-2024-38126, CVE-2024-38125, CVE-2024-38121, CVE-2024-38118, CVE-2024-38116, CVE-2024-38115, CVE-2024-29995, CVE-2024-38107, CVE-2023-40547, CVE-2024-38198, CVE-2024-38196, CVE-2024-38123, CVE-2022-2601.

QID: 92178 - Microsoft Windows Server Security Update for October 2024
CVE-2024-43611, CVE-2024-43593, CVE-2024-43549, CVE-2024-43453, CVE-2024-38262, CVE-2024-43607, CVE-2024-43592, CVE-2024-43589, CVE-2024-43575, CVE-2024-43567, CVE-2024-43564, CVE-2024-43545, CVE-2024-43544, CVE-2024-43521, CVE-2024-43512, CVE-2024-43456, CVE-2024-38212, CVE-2024-38265, CVE-2024-38124, CVE-2024-38129, CVE-2024-38029, CVE-2024-37979, CVE-2024-43608, CVE-2024-43541, CVE-2024-38261, CVE-2024-30092, CVE-2024-37976, CVE-2024-37982, CVE-2024-37983, CVE-2024-38149, CVE-2024-43501, CVE-2024-43506, CVE-2024-43513, CVE-2024-43511, CVE-2024-43509, CVE-2024-43514, CVE-2024-43515, CVE-2024-43516, CVE-2024-43517, CVE-2024-43518, CVE-2024-43519, CVE-2024-43520, CVE-2024-43535, CVE-2024-43532, CVE-2024-43534, CVE-2024-43547, CVE-2024-43550, CVE-2024-43551, CVE-2024-43554, CVE-2024-43556, CVE-2024-43560, CVE-2024-43562, CVE-2024-43563, CVE-2024-43565, CVE-2024-43570, CVE-2024-43572, CVE-2024-43573, CVE-2024-43583, CVE-2024-43599, CVE-2024-43615, CVE-2024-6197, CVE-2024-43553, CVE-2024-38179.

QID: 380615 - Mozilla Firefox and Firefox ESR Use-After-Free Vulnerability
(MFSA2024-51)
CVE-2024-9680

QID: 92121 - Microsoft Windows Security Update for March 2024
CVE-2024-21407, CVE-2024-21408, CVE-2024-21427, CVE-2024-21431, CVE-2024-21432, CVE-2024-21436, CVE-2024-21440, CVE-2024-21444, CVE-2024-21445, CVE-2024-21446, CVE-2024-21450, CVE-2024-26159, CVE-2024-26160, CVE-2024-26162, CVE-2024-26166, CVE-2024-26169, CVE-2024-26173, CVE-2024-26176, CVE-2024-26177, CVE-2024-26178, CVE-2024-26181, CVE-2024-26182, CVE-2024-26185, CVE-2024-26190, CVE-2024-21429, CVE-2024-21430, CVE-2024-21433, CVE-2024-21434, CVE-2024-21435, CVE-2024-21437, CVE-2024-21438, CVE-2024-21439, CVE-2024-21441, CVE-2024-21442, CVE-2024-21443,

CVE-2024-21451, CVE-2024-26174, CVE-2023-28746, CVE-2024-26161, CVE-2024-26197, CVE-2024-26170.

QID: 92139 - Microsoft Windows Security Update for May 2024
CVE-2024-29996, CVE-2024-29997, CVE-2024-29998, CVE-2024-29999, CVE-2024-30000, CVE-2024-30001, CVE-2024-30002, CVE-2024-30003, CVE-2024-30004, CVE-2024-30005, CVE-2024-30006, CVE-2024-30007, CVE-2024-30008, CVE-2024-30009, CVE-2024-30010, CVE-2024-30011, CVE-2024-30012, CVE-2024-30014, CVE-2024-30015, CVE-2024-30016, CVE-2024-30017, CVE-2024-30018, CVE-2024-30019, CVE-2024-30020, CVE-2024-30021, CVE-2024-30022, CVE-2024-30023, CVE-2024-26238, CVE-2024-29994, CVE-2024-30024, CVE-2024-30025, CVE-2024-30027, CVE-2024-30028, CVE-2024-30029, CVE-2024-30030, CVE-2024-30031, CVE-2024-30032, CVE-2024-30033, CVE-2024-30034, CVE-2024-30035, CVE-2024-30036, CVE-2024-30037, CVE-2024-30038, CVE-2024-30039, CVE-2024-30049, CVE-2024-30051, CVE-2024-30040, CVE-2024-30050.

QID: 92142 - Microsoft Windows Security Update for June 2024
CVE-2024-30099, CVE-2024-30097, CVE-2024-30096, CVE-2024-35265, CVE-2024-30095, CVE-2024-30094, CVE-2024-30093, CVE-2024-30091, CVE-2024-30090, CVE-2024-30089, CVE-2024-30088, CVE-2024-30087, CVE-2024-30086, CVE-2024-30085, CVE-2024-30084, CVE-2024-30083, CVE-2024-30068, CVE-2024-30067, CVE-2024-30066, CVE-2024-30065, CVE-2024-30064, CVE-2024-30063, CVE-2024-30062, CVE-2023-50868, CVE-2024-35250, CVE-2024-30082, CVE-2024-30080, CVE-2024-30078, CVE-2024-30077, CVE-2024-30076, CVE-2024-30075, CVE-2024-30074, CVE-2024-30072, CVE-2024-30070, CVE-2024-30069, CVE-2024-38213.

QID: 92158 – Microsoft Windows Domain Name System (DNS) Spoofing Vulnerability for August 2024
CVE-2024-37968

QID: 92169 - Microsoft Windows Security Update for September 2024
CVE-2024-38119, CVE-2024-38230, CVE-2024-38236, CVE-2024-38240, CVE-2024-38241, CVE-2024-38242, CVE-2024-38249, CVE-2024-38250, CVE-2024-38252, CVE-2024-38253, CVE-2024-38254, CVE-2024-38256, CVE-2024-43467, CVE-2024-38014, CVE-2024-38046, CVE-2024-38217, CVE-2024-38231, CVE-2024-38232, CVE-2024-38233, CVE-2024-38234, CVE-2024-38235, CVE-2024-38237, CVE-2024-38238, CVE-2024-38239, CVE-2024-38243, CVE-2024-38244, CVE-2024-38245, CVE-2024-38246, CVE-2024-38247, CVE-2024-38248, CVE-2024-38257, CVE-2024-38258, CVE-2024-38259, CVE-2024-38260, CVE-2024-38263, CVE-2024-21416, CVE-2024-38045, CVE-2024-43454, CVE-2024-43455, CVE-2024-43457, CVE-2024-43458, CVE-2024-43461, CVE-2024-43475, CVE-2024-30073, CVE-2024-43495, CVE-2024-43487.

QID: 38913 – SSH Prefix Truncation Vulnerability (Terrapin)
CVE-2023-48795

QID: 92183 - Microsoft Visual C++ Redistributable Installer Elevation of Privilege Vulnerability
CVE-2024-43590

QID: 379214 - Wireshark GVCP dissector crash Vulnerability (wnpa-sec-2024-01)
CVE-2024-0208

QID: 379215 - Wireshark Zigbee TLV dissector crash Vulnerability (wnpa-sec-2024-04)
CVE-2024-0210

QID: 379216 - Wireshark HTTP3 dissector crash Vulnerability (wnpa-sec-2024-03)
CVE-2024-0207

QID: 379217 - Wireshark DOCSIS dissector crash Vulnerability (wnpa-sec-2024-05)

CVE-2024-0211

QID: 379218 - Wireshark IEEE 1609.2 dissector crash Vulnerability (wnpa-sec-2024-02)
CVE-2024-0209

QID: 379315 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-01)
CVE-2024-0753, CVE-2024-0742, CVE-2024-0749, CVE-2024-0744, CVE-2024-0748, CVE-2024-0741, CVE-2024-0745, CVE-2024-0750, CVE-2024-0754, CVE-2024-0755, CVE-2024-0751, CVE-2024-0743, CVE-2024-0746, CVE-2024-0752, CVE-2024-0747.

QID: 379392 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-05)
CVE-2024-1551, CVE-2024-1548, CVE-2024-1555, CVE-2024-1556, CVE-2024-1547, CVE-2024-1546, CVE-2024-1549, CVE-2024-1557, CVE-2024-1550, CVE-2024-1554, CVE-2024-1553, CVE-2024-1552.

QID: 379518 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-12)
CVE-2024-2606, CVE-2024-2611, CVE-2024-2610, CVE-2024-2608, CVE-2023-5388, CVE-2024-2615, CVE-2024-2612, CVE-2024-2607, CVE-2024-2609, CVE-2024-2614, CVE-2024-2605, CVE-2024-2613.

QID: 379529 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-15)
CVE-2024-29944, CVE-2024-29943.

QID: 379541 - Wireshark T.38 dissector crash Vulnerability (wnpa-sec-2024-06)
CVE-2024-2955

QID: 379654 – Windows Secure Copy (WinSCP) Biased ECDSA Nonce Generation Vulnerability (CVE-2024-31497)
CVE-2024-31497

QID: 379655 – Putty (Pageant) Secret Keys Disclosure Vulnerability (CVE-2024-31497)
CVE-2024-31497

QID: 379667 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-18)
CVE-2024-3859, CVE-2024-3854, CVE-2024-3855, CVE-2024-3302, CVE-2024-3858, CVE-2024-3865, CVE-2024-3852, CVE-2024-3856, CVE-2024-3861, CVE-2024-3860, CVE-2024-3862, CVE-2024-3863, CVE-2024-3857, CVE-2024-3864, CVE-2024-3853.

QID: 379808 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-21)
CVE-2024-4775, CVE-2024-4777, CVE-2024-4367, CVE-2024-4770, CVE-2024-4771, CVE-2024-4778, CVE-2024-4768, CVE-2024-4772, CVE-2024-4765, CVE-2024-4769, CVE-2024-4766, CVE-2024-4774, CVE-2024-4773, CVE-2024-4776, CVE-2024-4767, CVE-2024-4764.

QID: 379936 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-25)
CVE-2024-5699, CVE-2024-5687, CVE-2024-5692, CVE-2024-5690, CVE-2024-5698, CVE-2024-5697, CVE-2024-5700, CVE-2024-5689, CVE-2024-5691, CVE-2024-5695, CVE-2024-5694, CVE-2024-5696, CVE-2024-5693, CVE-2024-5701, CVE-2024-5688.

QID: 380162 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-29)
CVE-2024-6615, CVE-2024-6601, CVE-2024-6603, CVE-2024-6606, CVE-2024-6608, CVE-2024-6602, CVE-2024-6609, CVE-2024-6613, CVE-2024-6612, CVE-2024-6614, CVE-2024-6610, CVE-2024-6611, CVE-2024-6605, CVE-2024-6607, CVE-2024-6604, CVE-2024-6600.

QID: 380175 - Wireshark SPRT dissector crash Vulnerability (wnpa-sec-2024-10)
CVEs = n/a

QID: 380283 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-33)
CVE-2024-8900, CVE-2024-7519, CVE-2024-7523, CVE-2024-7528, CVE-2024-7527, CVE-2024-7522, CVE-2024-7529, CVE-2024-7518, CVE-2024-7526, CVE-2024-7521, CVE-2024-7531, CVE-2024-7524, CVE-2024-7530, CVE-2024-7525, CVE-2024-7520.

QID: 380416 - Wireshark NTLMSSP dissector crash Vulnerability (wnpa-sec-2024-11)
CVE-2024-8250

QID: 380578 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-46)
CVE-2024-9395, CVE-2024-9397, CVE-2024-9392, CVE-2024-9394, CVE-2024-9396, CVE-2024-9402, CVE-2024-9391, CVE-2024-9401, CVE-2024-9393, CVE-2024-9403, CVE-2024-9398, CVE-2024-9400, CVE-2024-9399.

QID: 380669 - Wireshark AppleTalk and RELOAD Framing dissector crash Vulnerability (wnpa-sec-2024-13)
CVEs = n/a

QID: 380688 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-53)
CVE-2024-9936

QID: 380793 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-55)
CVE-2024-10467, CVE-2024-10461, CVE-2024-10468, CVE-2024-10466, CVE-2024-10463, CVE-2024-10459, CVE-2024-10465, CVE-2024-10460, CVE-2024-10462, CVE-2024-10458, CVE-2024-10464.

QID: 92116 - Microsoft Windows Domain Name System (DNS) Server Denial of Service (DoS) Vulnerability for February 2024
CVE-2023-50387

QID: 92130 - Microsoft .NET Framework Update for April 2024
CVE-2024-21409

QID: 92150 - Microsoft .NET Framework Update for July 2024
CVE-2024-38081

QID: 92176 - Microsoft .NET Framework Update for October 2024
CVE-2024-43483, CVE-2024-43484

QID: 379302 - Windows Secure Copy (WinSCP) Security Update
CVE-2023-48795

QID: 379830 - Wireshark MONGO and ZigBee TLV dissector infinite loops Vulnerability (wnpa-sec-2024-07)
CVE-2024-4854

QID: 380508 – Libcurl Denial of Service (DoS) Vulnerability
CVE-2024-7264

QID: 379828 - Wireshark Editcap byte chopping crash Vulnerability (wnpa-sec-2024-08)
CVE-2024-4853

QID: 379829 - Wireshark Editcap secret injection crash Vulnerability (wnpa-sec-2024-09)
CVE-2024-4855

QID: 380428 - Mozilla Firefox Multiple Vulnerabilities (MFSA2024-39)
CVE-2024-8386, CVE-2024-8382, CVE-2024-8381, CVE-2024-8387, CVE-2023-6870, CVE-2024-8388, CVE-2024-8384, CVE-2024-8385, CVE-2024-8383, CVE-2024-8389.

Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://download.avaya.com/css/public/documents/101081871

Avaya PDU Router (Linux):

Severity/risk level: **High/Critical**

Avaya PDU Router 5.0.0.0.13

This new PDU Router build 5.0.0.0.13 includes security fixes to critical/high/medium vulnerabilities identified on previous PDU Router versions up to **November 12th, 2024**. Any newer vulnerabilities identified after cutover date will be addressed in the next release.

Vulnerabilities mitigated:
RHSA-2024:7700, CVE-2024-8900, CVE-2024-9392, CVE-2024-9393, CVE-2024-9394, CVE-2024-9396, CVE-2024-9397, CVE-2024-9398, CVE-2024-9399, CVE-2024-9400, CVE-2024-9401, CVE-2024-9402, RHSA-2024:7977, CVE-2024-9680, RHSA-2024:8038, CVE-2023-45290, CVE-2024-34155, CVE-2024-34156, CVE-2024-34158, RHSA-2024:8729, CVE-2024-10458, CVE-2024-10459, CVE-2024-10460, CVE-2024-10461, CVE-2024-10462, CVE-2024-10463, CVE-2024-10464, CVE-2024-10465, CVE-2024-10466, CVE-2024-10467, RHSA-2024:7848, CVE-2024-5535.

Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://download.avaya.com/css/public/documents/101081871

HPE Nimble CS1000 Storage Array:

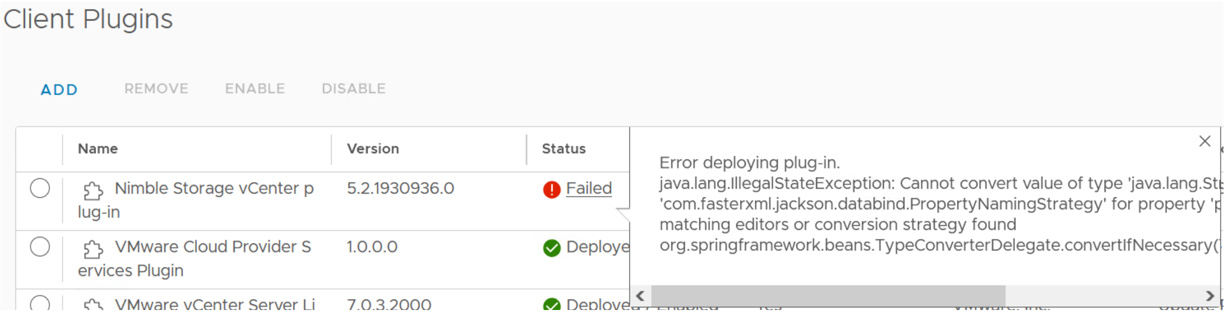
Severity/risk level: **Medium**

NimbleOS/Alletra Software Release HPE-Alletra-6.1.2.502-1057650

If the July 2024 SSP has already been fully installed, the new NimbleOS SW can be downloaded from PLDS individually:
File: ASP4200_5.0_HPE-Alletra-6.1.2.502-1057650-opt.update.v2 - PLDS ID: **CPOD0000267**

CVEs/Vulnerabilities mitigated: N/A
Fixes in this new release applicable to ASP 4200 solution (Fixes are cumulative in NimbleOS/Alletra releases):

- COLLABPOD-3636 | HPE Nimble plugin for vCenter is unavailable/failed after upgrade to vCenter 7.0u3q or later releases.



Client Plugins

	Name	Version	Status
○	Nimble Storage vCenter plug-in	5.2.1930936.0	Failed
○	VMware Cloud Provider Services Plugin	1.0.0.0	Deploye
○	VMware vCenter Server Li	7.0.3.2000	Deploye

```
Error deploying plug-in.
java.lang.IllegalStateException: Cannot convert value of type 'java.lang.St
'com.fasterxml.jackson.databind.PropertyNamingStrategy' for property 'p
matching editors or conversion strategy found
org.springframework.beans.TypeConverterDelegate.convertIfNecessary(
```

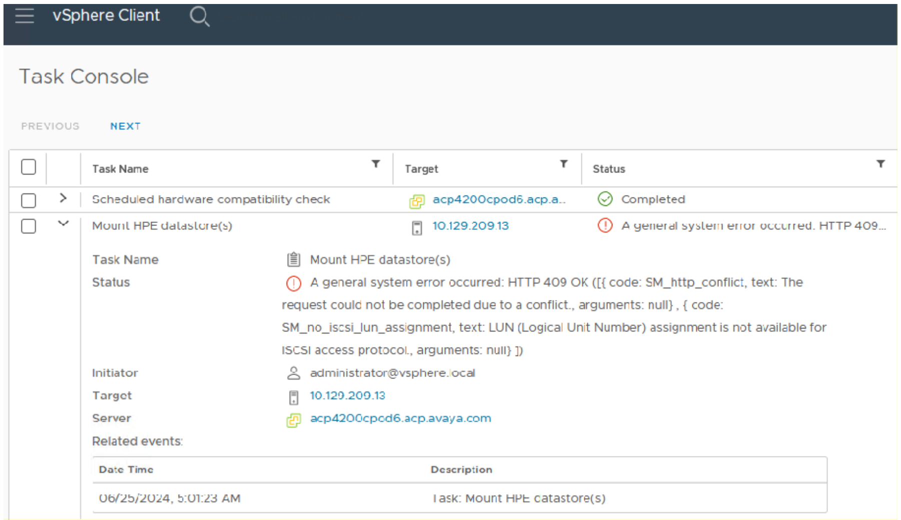
- Vendor JIRA: AS-186023

HPE Issue Description:

HPE Services - Storage Support has detected a compatibility issue starting with vCenter 7.0u3q (Build: 23788036) and later that will lead to the HPE Storage vCenter plugin being non-functional after a vCenter update to version 7.0u3q (Build: 23788036) or later. This is tracked under AS-186023.

AS-186023 - HPE Storage vCenter Plugin fails to load on 7.0.3.01900-23788036 (7.0U3q) or later. In this release, VMware has upgraded a dependency that breaks the HPE Storage vCenter plugin integration. This issue is observed both when the user updates vCenter to this or any later version of 7.0 or when the user does a new deployment with this vCenter version.
For more details see HPE's Support Alert/Customer Advisory:
https://support.hpe.com/hpesc/public/docDisplay?docId=a00142228en_us&docLocale=en_US
For more details see VMware/Broadcom KB article: https://knowledge.broadcom.com/external/article/371270/post-vc-upgrade-nimble-plugin-deployment.html

- COLLABPOD-3632 | Unable to mount or create VMFS volumes using the Nimble vCenter Plugin.



□		Task Name	Target	Status
□	>	Scheduled hardware compatibility check	acp4200cpod6.acp.a...	Completed
□	⌄	Mount HPE datastore(s)	10.129.209.13	A general system error occurred. HTTP 409...

Task Name: Mount HPE datastore(s)
Status: A general system error occurred: HTTP 409 OK ([{ code: SM_http_conflict, text: The request could not be completed due to a conflict., arguments: null} , { code: SM_no_iscsi_lun_assignment, text: LUN (Logical Unit Number) assignment is not available for ISCSI access protocol., arguments: null}])
Initiator: administrator@vsphere.local
Target: 10.129.209.13
Server: acp4200cpod6.acp.avaya.com
Related events:

Date Time	Description
06/25/2024, 5:01:23 AM	Task: Mount HPE datastore(s)

- Vendor JIRA: AS-180001

Issue Description:

When Volume Scoped Target (VST) is enabled, the Host Bus Adapter static discovery will not have the array group path in it, which causes datastore creation using the vCenter plugin to fail.

Note: New installations of the array OS 5.1.x or later will use Group Scoped Target (GST). If you upgrade to 5.1.x or later the default target will continue to use VST. Not every array in the field will have VST configured, thus not every system will be impacted, nonetheless, Avaya is making this new Nimble OS General Availability as part of this July 2024 which will require upgrading every array in the field to comply with the July 2024 SSP software baseline.

For further information about Group Scoped Target reference to vendor article: Online Help 6.0.0.0 - Group Scoped iSCSI Target (hpe.com)

See the release notes for more details: NimbleOS_Release_Notes_Array_OS_6.1.2.502.pdf (hpe.com)

Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://download.avaya.com/css/public/documents/101081871

Warning: Array must be running NimbleOS 6.0.0.300 (from R5.0 baseline) or later to update directly to NimbleOS 6.1.2.502.

Dell/EMC VNXe3200 Storage Array:

Severity/risk level: **High/Critical**

Software Release v3.1.17.10229825 (Still the latest from previous SSP releases)

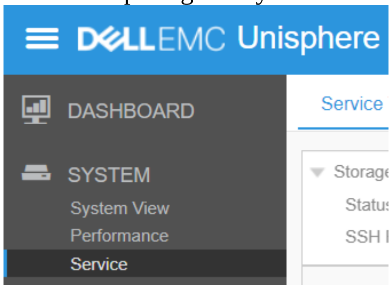
Download the May 2024 or July 2024 SSP ZIP file for the VNXe3200 **v3.1.17.10229825** software.
PLDS ID CPOD0000259 – ASP4200_5.0.x_Infrastructure_Security_Service_Pack_July2024_v2.zip
PLDS ID CPOD0000266 – ASP4200_5.0.x_Infrastructure_Security_Service_Pack_May2024.zip
Important: Please note that this is v3.1.17 but it's a different build number than the previous release (3.1.17.**10223906**)

CVEs/Vulnerabilities mitigated & bug fixes: Security and Unisphere enhancements in this release.
VNXe3200-3.1.17.10229825-Release-Notes (dell.com)
Upgrade instructions: See PSN005974u for the upgrade procedure.

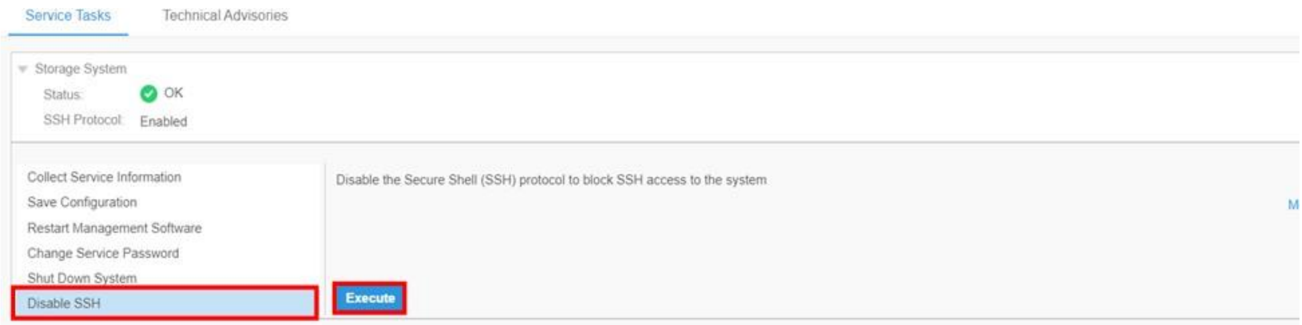
Workaround procedure to mitigate vulnerability CVE-2018-15473:

Note: Upgrade the VNXe3200 Storage Array to release 3.1.17 first before proceeding with the following workaround. At the time this version of the PSN was published, there is no permanent fix made available by our vendors.

1. From the MSC, open a web browser to the IP/FQDN of the array and log in with the admin credentials. See the customer workbook for login details.
2. On the left pane go to System > Service



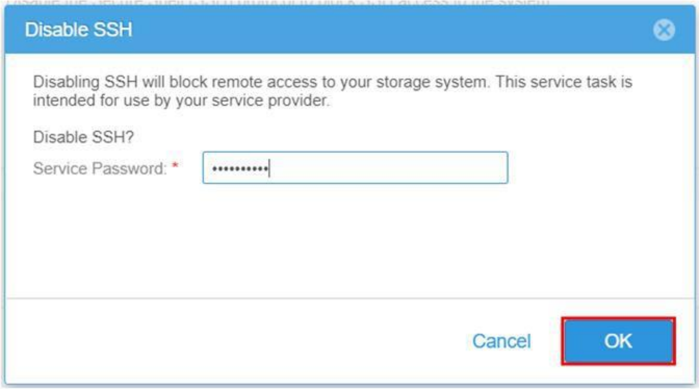
3. Under the Service Tasks tab select Disable SSH > Execute



Status: OK
SSH Protocol: Enabled

Disable the Secure Shell (SSH) protocol to block SSH access to the system

4. Enter the Service Password and click OK. SSH is now Disabled.



Disabling SSH will block remote access to your storage system. This service task is intended for use by your service provider.

Disable SSH?

Service Password: * ••••••••••

Verification

N/A

Failure

Contact Avaya Support in case there is any issue or failure.

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 to the individual component sections in this PSN for specific CVE vulnerability details and information.

Avaya Security Vulnerability Classification

Medium

Mitigation

Reference to the procedure section 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.