

PSN # PSN028007u

Original publication date: 21-Dec-2022. This is Issue #08, published date: 01-Sept-2023. Severity/risk level Medium Urgency When Convenient

Name of problem

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, Dell/EMC VNXe3200, 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

UPDATE 09/01/2023

Updated version (v2) of the July SSP ZIP file. New file name: ASP4200_5.0.x_Infrastructure_Security_Service_Pack_July2023-v2.zip
With v2, the HPE Gen10v1/v2 **B4** SPP ISO file has been removed and replaced with the HPE Gen10v1/v2 **B5** SPP ISO file. See section “HPE DL360 Gen9/Gen10v1/Gen10v2 Servers – Service Pack for ProLiant (SPP)” for more details.
No change in the remainder of the SW/FW files from previous July SSP ZIP.

UPDATE 08/01/2023

Added support to ESXi Quick Boot feature – See the VMware section for further information.

UPDATE 7/26/2023

New zip file - ASP4200_5.0.x_Infrastructure_Security_Service_Pack_July2023.zip.
New individual PLDS IDs for the MSC, AO and PDU Router files.

This July 2023 update to the security service pack includes the following new SW/FW:

- VMware vCenter 7.0 U3m build 21784236.
- VMware ESXi 7.0 U3m Build 21686933
- HPE DL360 Gen10v1/v2 Server FW SPP version B4
- HPE DL360 Gen9 Server FW SPP version B3
- HPE DL360 G9 iLO firmware v2.82 (bin file)
- HPE Nimble/Alletra version 6.1.1.200-1020304
- VSP 7400 VOSS v8.10.0.

- Avaya Management Server Console (MSC) 5.0.0.0.13
- Avaya Orchestrator (AO) 1.5 build 51
- Avaya PDU router v5.0.0.0.7

UPDATE 3/14/2023

New Avaya PDU router v5.0.0.0.3 available for install. Individual PLDS ID created for the OVA file and a new “Avaya PDU Router (Linux)” section created to cover RHSAs mitigated.

UPDATE 2/8/2023

Updated the Supported Upgrade Paths table and added a new section covering partially supported upgrades from R4.1.0.1 with **11/08/2022** Security Service Pack to this R5.0 Jan 2023 SSP.

New Avaya Orchestrator 1.5 build 50 release. New ISO and OVA PLDS IDs added and updates to AO 1.5 section.

UPDATE 2/6/2023

Updated the problem description and patch installation instructions sections to capture user attention on important upgrade supportability statements.

UPDATE 1/31/2023

The updated version of the zip file PLDS ID CPOD0000247

ASP4200_5.0.x_Infrastructure_Security_Service_Pack_Jan2023.zip. See the *VMware* section for more details. No other changes to the firmware/software in the new .zip file.

- Support of vCenter 7.0 U3j Build 20990077
- Support of ESXi 7.0 U3i Build 20842708

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 **CPOD0000252** – ASP4200_5.0.x_Infrastructure_Security_Service_Pack_July2023-**v2**.zip

Note: This updated ZIP file (v2) replaces the “ASP4200_5.0.x_Infrastructure_Security_Service_Pack_July2023.zip” file released on 7/26/23.

Upgrade FW/SW files included in the ZIP file:

- ***New*** bp-avaya-dl360g10-ASP4200-5-0-0-B5.iso
- HPE-Alletra-6.1.1.200-1020304-opt.update.v2
- ilo4_282.bin
- bp-avaya-dl360g9-ASP4200-5-0-0-B3.iso
- VMware-HPE-ESXi-7.0U3m-21686933.zip
- VMware-vCenter-Server-Appliance-7.0.3.01500-21784236-patch-FP.iso
- VMware-VCSA-all-7.0.3-21784236.iso
- VOSS7400.8.10.0.0.tgz
- VNxe-3.1.17.10229825.tgz.bin.gpg (**Please note that this is v3.1.17 but it's a different build# than the previous release**)
- pro-v80x.bin
- amshelpComponent_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:

- 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):

Note: One OVA is for MSC deployment within VMware 7.0. One OVA is for MSC deployment within VMware 6.5 before upgrading to VMware 7.0.

- Avaya Management Server Console 5.0.0.0.13-esxi7.ova – PLDS ID: **CPOD0000255**
- Avaya Management Server Console 5.0.0.0.13-esxi65.ova – PLDS ID: **CPOD0000256**

Avaya PDU Router (Linux):

- Avaya PDU Router 5.0.0.0.7.ova – PLDS ID: **CPOD0000257**

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.

Supported Upgrade Paths:

From ASP 4200 Release	To ASP 4200 5.0 SSP (July 2023)
R4.x	Not Supported – DO NOT attempt, upgrade will fail.
R4.1.0.1 with 11/08/2022 Security Service Pack ONLY (Issue 14)	Partially Supported – Gen9/Gen10 Server Firmware ONLY. See section below this table for special instructions.
R5.0	Supported
R5.0 + SSP from Dec 2022	Supported
R5.0 + SSP from Jan 2023	Supported (Important Gen9 Server FW change – See note in corresponding section.) (Important vCenter update procedure change – See observations and known issues in corresponding section.)

Upgrade support from ASP 4200 4.1.0.1 on latest 11/08/2022 Security Service Pack:

There is partial upgrade support for customers that are on the latest ASP 4200 4.1.0.1 Security Service Pack released on **11/08/2022 ONLY** (Issue 14). Due to the R4.1.0.1 latest Security Service Pack being released after R5.0 GA and having newer firmware for the Gen9 and Gen10v1/v2 servers, there is no step-up upgrade required for server firmware, however, there are special instructions that must be conducted in order to eliminate any impacts.

High-level Instructions

Reference the latest MSC upgrade documentation for the procedures.

<https://download.avaya.com/css/public/documents/101081871>

Confirm that the latest ASP 4200 4.1.0.1 SSP from 11/08/2022 is installed. See PSN005800u to confirm before beginning: <https://download.avaya.com/css/public/documents/101074130>

1. Pre-requisites:

- Confirm that the server firmware is first on the Gen9 B6 and/or Gen10 B6 firmware. Expected firmware versions before conducting the high-level steps below:

○ Gen9 B6 Server firmware versions

Name	Version
HPE Integrated Lights-Out 4	2.81
HPE Broadcom NX1 Firmware for 1Gb 331i NIC card	2.29.0 (HPE v20.19.51) BC 1.46
HPE QLogic NX2 Firmware for 10Gb 534FLR NIC card	2.29.2 (HPE v7.18.82) MFW 7.16.03
HPE Smart Array and Smart HBA H240ar, H240nr, H240, H241, H244br, P240nr, P244br, P246br, P440ar, P440, P441, P542D, P741m, P840, P840ar, and P841	7.00
HPE ProLiant DL360 Gen9 (P89) Server BIOS	3.02 2022 07 18

○ Gen10 B6 Server firmware versions

Name	Version
HPE Integrated Lights-Out 5	2.72
HPE Broadcom NX1 Firmware for 1Gb 331i NIC card	2.29.0 (HPE v20.19.51) BC 1.46
HPE QLogic NX2 Firmware for 10Gb 534FLR NIC card	2.29.2 (HPE v7.18.82) MFW 7.16.03
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	5.32(B)
HPE ProLiant DL360 Gen10 (U32) Server BIOS	2.68_2022_07_14

IMPORTANT: If the server is not on the firmware listed above, the server is not on the latest 4.1.0.1 SSP release and the following procedure is not applicable or supported.

2. Pre-upgrade to R5.0:

- Upgrade the vCenter Server to 7.0 U3c (from R5.0)
- Upgrade to ESXi 7.0 U3c (from R5.0)
- Install all other components SW/FW from the initial 5.0 release. (*Don't need to install the Gen9 B1 FW*)

or Gen10 B1/B2 FW from the initial 5.0 release)

3. Upgrade to R5.0 SSP July 2023:

- Install the Gen9 B3 and/or Gen10 B5 firmware.
 - Gen9 FW ISO – **bp-avaya-dl360g9-ASP4200-5-0-0-0-B3.iso** (from R5.0 SSP July 2023)
 - Gen10 FW ISO – **bp-avaya-dl360g10-ASP4200-5-0-0-0-B5.iso** (from R5.0 SSP July 2023 – v2 file released in Sept 2023)
- Upgrade to vCenter Server 7.0 U3m (from R5.0 SSP July 2023)
- Upgrade to ESXi 7.0 U3m (from R5.0 SSP July 2023)
- Install all other components SW/FW

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 in order to mitigate severity 4 and 5 vulnerabilities for SNMPv2.

HPE DL360 Gen9/Gen10v1/Gen10v2 Servers – Service Pack for ProLiant (SPP):

IMPORTANT:

Avaya is working closely with our 3rd party vendor, HPE to understand the availability and supportability of the latest HPE DL360 Gen9 BIOS versions 3.04 and 3.08. They have been removed from the vendor website as those versions were not meant to be provided to general customers.

In the January SPP release, the Gen9 ISO file (B2) included BIOS version 3.04. After further discussions with HPE Management and Engineering teams, customers that have already installed v3.04 from our January release will continue to be supported. No new installs of v3.04 will be supported by our vendor.

Customers that have not upgraded to the January release will instead need to install the Gen9 B3 SPP ISO included in this July release. **This will include BIOS 3.02 and iLO 2.82.**

iLO release for Gen9 server:

Important: For customers that already have the January SSP installed (BIOS 3.04, iLO 2.81), only the iLO FW requires upgrade, installing the Gen9 B3 FW is not required. For customers that have not installed the January SSP, no action is required as the B3 SPP ISO file includes iLO 2.82.

➤ Gen9 iLO BIN file: ilo4_282.bin

Installation instructions: Refer to the existing procedure in [PSN005312u](#) to upgrade to v2.82 via the iLO UI.

New Gen10 v1/v2 SPP iso image:

- Gen10v1/v2 SPP file: bp-avaya-dl360g10-ASP4200-5-0-0-0-B5.iso

When upgrading the G10 v1/v2 FW from the SPP B1 version (ASP4200 R5.0) to the B4 version (July 2023 SSP) an additional reboot of the compute server was observed when upgrading the RAID controller FW. This additional reboot was occurring after the initial FW upgrade was completed and ESXi was up, which could potentially lead to a service impact.

Third party vendor did not notify the change in the way the FW for the raid controller is upgraded if using a .fwpkg file in the SPP. The B4 FW ISO included a .fwpkg for the raid controller. With the B5 SPP ISO this is avoided by using the individual rpm instead of the .fwpkg file to get the raid controller updated to the desired FW version.

If previous G10 B4 SPP file “bp-avaya-dl360g10-ASP4200-5-0-0-0-B4.iso” has already been installed, there is no action required. The G10 B5 ISO **does not have any newer FW included**, it only has an internal fix to prevent servers from unexpectedly rebooting while the raid controller is getting upgraded.

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

Gen9 SPP iso image:

Important: This is only applicable for customers that have not upgraded to the January SSP release.

- Gen9 SPP file: bp-avaya-dl360g10-ASP4200-5-0-0-0-B3.iso

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

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

Contents of HPE Gen10v1/v2 SPP image (B5):

Name	Version	CVEs mitigated / Bug fixes
HPE Integrated Lights-Out 5	2.81	No vulnerabilities. Includes bug fixes.
HPE Broadcom NX1 Firmware for 1Gb 331i NIC card	2.32.3 (HPE v20.24.41) BC 1.46	No vulnerabilities. Includes enhancements and bug fixes.
HPE QLogic NX2 Firmware for 10Gb 534FLR NIC card	2.32.0 (HPE v7.19.14) MFW 7.16.13	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	5.61c	No vulnerabilities. Includes enhancements.
HPE ProLiant DL360 Gen10 (U32) Server BIOS	2.80_2023_04_20	CVE-2022-38087. Includes bug fixes.

Contents of HPE Gen9 SPP image (B3):

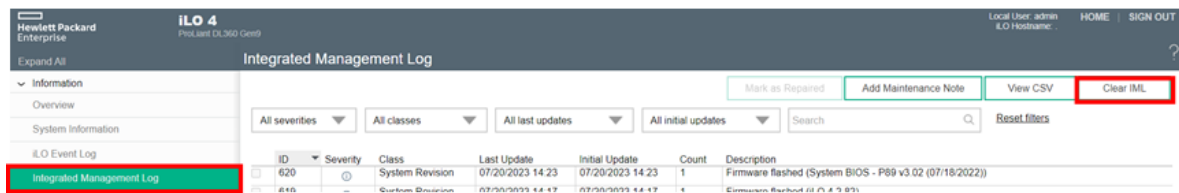
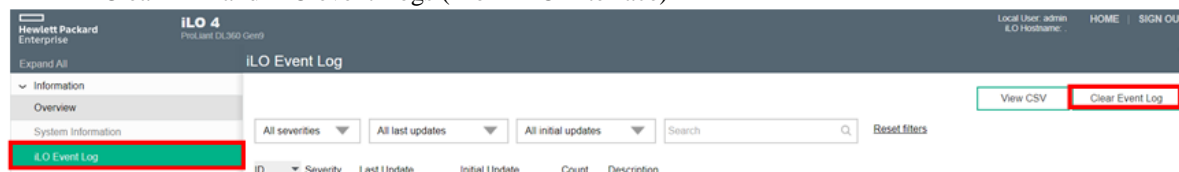
Name	Version	CVEs mitigated / Bug fixes
HPE Integrated Lights-Out 4	2.82	No vulnerabilities. Includes bug fixes.
HPE Broadcom NX1 Firmware for 1Gb 331i NIC card	2.29.0 (HPE v20.19.51) BC 1.46	No vulnerabilities. Includes bug fixes.
HPE QLogic NX2 Firmware for 10Gb 534FLR NIC card	2.30.2 (HPE v7.19.02) MFW 7.16.05	No vulnerabilities. Includes bug fixes.
HPE Smart Array and Smart HBA H240ar, H240nr, H240, H241, H244br, P240nr, P244br, P246br, P440ar, P440, P441, P542D, P741m, P840, P840ar, and P841	7.20	No vulnerabilities. Includes bug fixes.
HPE ProLiant DL360 Gen9 (P89) Server BIOS	3.02_2022_07_18	No vulnerabilities. Includes bug fixes.

Observations and known issues:

- ****NEW**** 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.
- ****NEW**** When running the Gen9 B3 firmware upgrade some of the firmware may not install and will require rerunning the SPP a second time in order to upgrade. If the firmware still does not install after rerunning the SPP, please reach out to Avaya Support for assistance with a manual mode install. See additional high-level checks below.

High-level troubleshooting steps:

- Ensure latest Windows Server 2019 MSC from R5.0 is installed.
- Clear IML and iLO event Logs (From iLO Interface)



- Reset iLO interface (From iLO interface)

The screenshot shows the iLO 4 Diagnostics page for a ProLiant DL360 Gen9. The left sidebar has 'Diagnostics' highlighted. The main content area shows 'iLO Self-Test Results' with a green 'iLO Health' status. A table lists various self-test components, all with a status of 'Pass'. Below the table, there is a 'Reset iLO' section with a warning message and a 'Reset' button highlighted with a red box.

Self-Test	Status	Notes
Power Management Controller	Pass	Version 1.0.9
CPLD - PAL0	Pass	ProLiant DL360 Gen9 System P
CPLD - PAL1	Pass	ProLiant DL360 Gen9 SAS Prog
BMC USB Interface	Pass	
NVRAM data	Pass	
NVRAM space	Pass	
Embedded Flash/SD-CARD	Pass	Controller firmware revision 2.10
EEPROM	Pass	
Host ROM	Pass	
Supported host	Pass	

- Conduct a full power cycle to the server, allowing 5 minutes before plugging back the power cords.

Reach out to Avaya Support if problem still persist.

- 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

The screenshot shows the VMware ESXi boot order. The 'Embedded RAID 1: HPE Smart Array P408i-a SR Gen10 - 279.3 GiB, RAID1 Logical Drive 1 (Target:0, Lun:0)' is highlighted with a red box, indicating it is the second item in the boot order.

Server boot order after firmware upgrade:

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

Server Boot Order

The screenshot shows the VMware ESXi boot order after the firmware upgrade. The 'Embedded RAID 1: HPE Smart Array P408i-a SR Gen10 - 279.359 GiB, RAID1 Logical Drive 1 (Target:0, Lun:0)' is highlighted with a red box, indicating it is now the last item in the boot order.

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 :

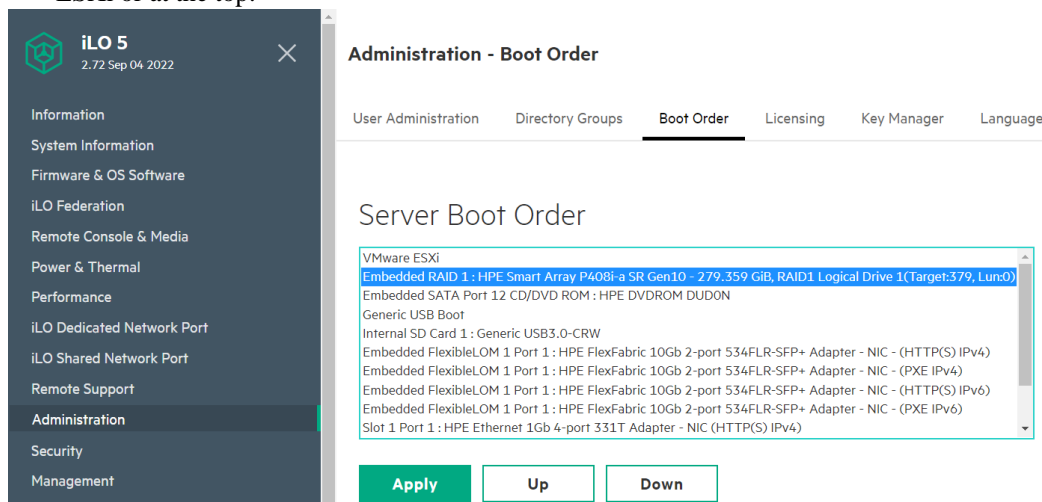

```
>> Booting Embedded FlexibleLOM 1 Port 1 : HPE FlexFabric 10Gb 2-port 534FLR-SFP
+ Adapter - NIC - (HTTP(S) IPv4)
```

```
>> 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.



- Click Apply to save the changes.

VMware:

VMware vCenter Server 7.0 U3m build 21784236

CVEs/Vulnerabilities mitigated: CVE-2023-20892, CVE-2023-20893, CVE-2023-20894, CVE-2023-20895, CVE-2023-20896. Includes bug fixes as well as fixes for previous known issues and vulnerabilities.

<https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-vcenter-server-70u3m-release-notes/index.html>

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


Observations and known issues:

- ****NEW**** 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.

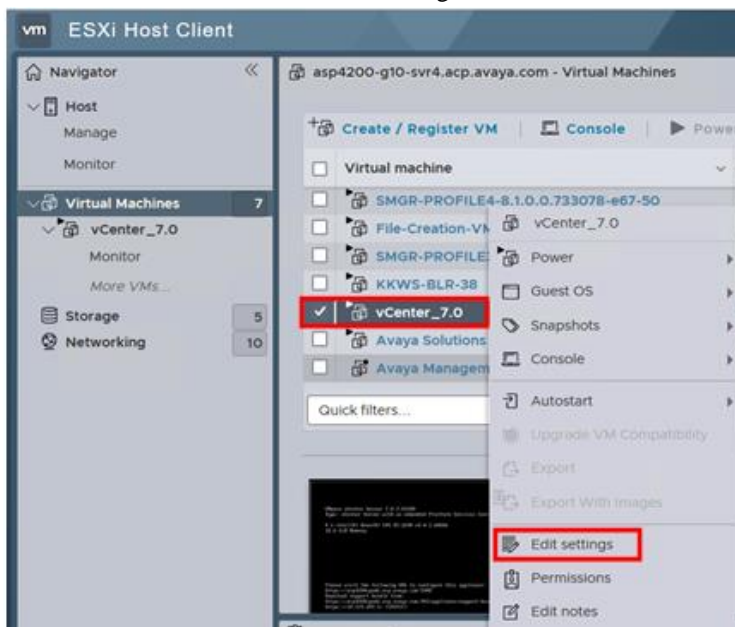
IMPORTANT: VMware Engineering is currently working this request and has not provided an ETA on a permanent fix at the time this July PSN update was released. Due to this issue, there is a new procedure to update the vCenter with the patch ISO.

Updating the vCenter Server Appliance:

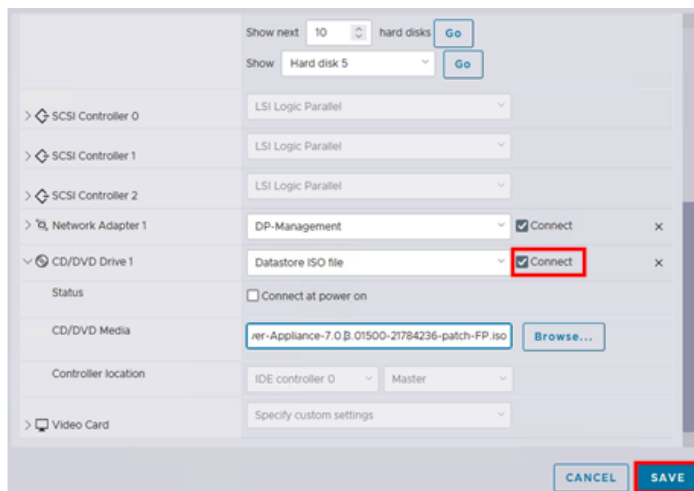
1. Connect to the MSC and log in using the Administrator account.
2. Open a web browser and enter the URL for the vSphere Web Client:
https://vcenter_server_ip_address_or_fqdn/ui. Login using the administrator@vsphere.local account.
3. Click on the  icon and select storage.
4. From the menu on the left,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

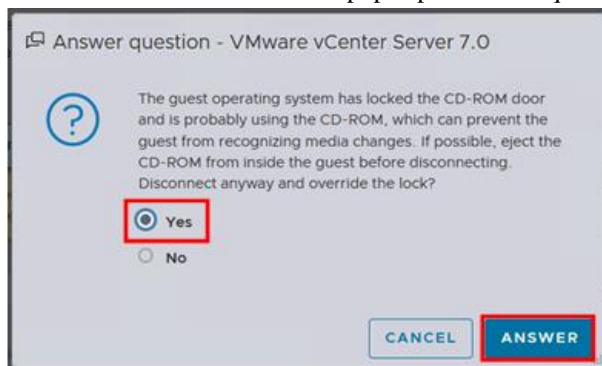
8. Click on the  icon to go to the Hosts and Clusters view. Locate the vCenter VM and from the summary tab take note of the ESXi host that its located on.
9. Open a new browser tab and go to the ESXi host that the vCenter VM is located. Login with the root credentials.
10. Go to Virtual Machines and select and right click the vCenter VM. Go to Edit Settings.



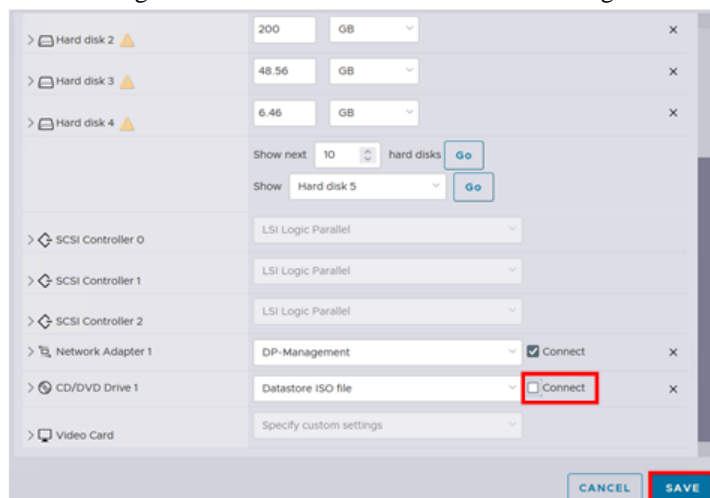
11. From the CD/DVD drive 1 option, select datastore ISO from the dropdown menu.
12. If not already, expand the CD/DVD drive 1 view and click browse.
13. Navigate to and select the VCSA update patch ISO file uploaded during step 6 and click Select to mount it to the vCenter VM CD/DVD drive.
14. Ensure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



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



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 Connect 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 (7.0.3.01500).
21. Click Stage and Install.
22. Accept the license agreement and click Next.
23. Check that a back up 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 (7.0.3.01500).

VMware/HPE ESXi 7.0 U3m build 21686933

This ESXi release is customized by Avaya to include ESXi 7.0 U3m with updated HPE add-on version 703.0.0.11.3.0.5 from April 2023.

CVEs/Vulnerabilities mitigated: Includes critical bug fixes as well as fixes for previous known issues and vulnerabilities.

Note: The roll-up bulletins contain the latest VIBs with all the fixes since the initial release of ESXi 7.0.

<https://docs.vmware.com/en/VMware-vSphere/7.0/rn/vsphere-esxi-70u3m-release-notes.html>

Important: VMware ESXi 7.0 U3c build 19193900 upgrade ISO file from initial Release 5.0 or ESXi 7.0 U3i build 20842708 from the previous SSP **must be** installed before or in parallel to upgrading to the ESXi 7.0 U3m patch release, no direct upgrade from ASP 4200 4.x release to this new 5.0 SSP. See the supported upgrade paths table above for more details.

vSphere Quick Boot

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: VMware-HPE-ESXi7.0-U3-21686933

Name	ID	Severity	Type	Category	ESXi Version	Impact	Vendor	Release Date
Image Profile VMware-HPE-ESXi7.0-U3m-21686933	VMware-HPE-ESXi7.0-U3m-21686933	Moderate	Rollup	Other	7.0.3	Reboot, Maintenance Mode	VMware, Inc. / HPE	05/17/2023, 8:00:00 PM

Rollup Bulletin

Bulletin ID	Category	Severity
ESXi70U3m-21686933	Bugfix	Critical

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

Enabling Quick Boot in vLCM

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

Remediate | 10.1.1.1 with ASP 4200 5.0 July 2023 SSP ×

✓ 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

<input checked="" type="checkbox"/>	Host Name	Version	Patches	Extensions	Remediation Status
<input checked="" type="checkbox"/>	10.1.1.1	7.0.3	0 (0 Staged)	0 (0 Staged)	✓ Ready

☒ 1 [EXPORT](#) 1 Hosts

> Install

> Scheduling Options: Will remediate immediately

✓ Remediation settings

CANCEL

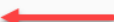
REMEDiate

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

> Scheduling Options: Will remediate immediately

▼ Remediation settings

CLOSE DIALOG AND GO TO 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 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	<input checked="" type="checkbox"/> 
Check host health after installation	<input checked="" type="checkbox"/>
Ignore warnings about unsupported hardware devices	<input type="checkbox"/>

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

CANCEL REMEDIATE

- Proceed with the remediation process as instructed in the latest MSC upgrade document <https://download.avaya.com/css/public/documents/101081871>
- Note:** Quick boot is disabled by default, and it must be enabled every time a host or cluster remediation is conducted. Alternatively, this feature can be enabled at the Lifecycle Manager-Baseline Remediation level. Follow below steps to enable quick boot globally:
- 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.

vSphere Client

Lifecycle Manager | ACTIONS

Image Depot Updates Imported ISOs Baselines Settings

Administration
Patch Downloads
Patch Setup

Host Remediation
Images
Baselines
VMs

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

EDIT

- 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

CANCEL
SAVE

Ologic, AMS, and Storage Controller Drivers:

QLogic 10Gb qfle3 driver update version 1.4.35.0 (**NOTE: The qfle3 driver is part of the ESXi 7.0 U3m patch. No action needed for this July SSP release**)

STOP! - IMPORTANT: Before beginning the qfle3 driver update to the latest version 1.4.35.0, 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.

Updated Qfle3 driver to be installed after 10Gb NIC firmware upgrade included in the SPP in this PSN.

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: **7.16.13**
Driver Version: **1.4.35.0**

For Gen9 servers - After both firmware and driver updates, the following should be observed when running the network commands on vmnics:

MFW/Firmware: **7.16.5**
Driver Version: **1.4.35.0**

Agentless Management Service (AMS)

Gen9 AMS version **11.8.5.8-1**

Gen10 AMS version **11.9.0.9-1** (Installed via the ESXi 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** (Installed via the ESXi patch)

Gen10 Storage Controller version **70.4380.0.108** (Installed via the ESXi 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>

Avaya Orchestrator 1.5

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>

Switches:

VSP7400 network switches VOSS 8.10.0.0

For upgrade instructions, reference [PSN028006u](#).

Validated upgrade path:

- 8.9.x to 8.10.0
- 8.8.x to 8.10.0

Warning:

VOSS FW 8.10.0.0 is not supported on the VSP 7200 switches with the ASP4200 Solution. **DO NOT** attempt to upgrade the VSP 7200 switches to VOSS 8.10.0.0 as **this is not supported**.

CVEs/Vulnerabilities mitigated: Includes bug fixes and incorporates all fixes from prior releases.

https://documentation.extremenetworks.com/release_notes/VOSS/810/downloads/ReleaseNoteVOSS_8.10_RN.pdf

PDU:

Sentry4 PDU version v80x (Still the latest from the Jan SSP release)

CVEs/Vulnerabilities mitigated: CVE-2022-0778. This is a 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 v80x, a message is displayed in the UI recommending user to install a CA-signed certificate instead of using the self-signed certificate.

The screenshot displays the web interface of a Sentry Switched PDU. On the left is a navigation menu with 'Server Technology' at the top, followed by 'Overview', 'System' (highlighted), 'Monitoring', 'Control', and 'Configuration'. The main content area has a blue header with 'PROB Sentry Switched PDU PIPS'. Below this is a red warning message: 'To improve security, consider uploading a trusted server identity certificate instead of the default self-signed factory certificate.' A green arrow points to this message. Under the 'Overview' section, there is a 'System information' table with the following data:

Firmware:	Sentry Switched PDU Version 8.0x
Uptime:	15 days 21 hours 25 minutes 39 seconds
Ethernet NIC S/N:	9640243
Active Users:	1

Avaya Management Server Console (MSC):

Avaya Management Server Console 5.0.0.13

This new MSC build 5.0.0.13 includes security fixes to multiple vulnerabilities identified on previous MSC versions up to **July 1st, 2023**. Any newer vulnerabilities identified after cutover date will be addressed in the next release.

Vulnerabilities mitigated:

QID: 378332 - Microsoft WinVerifyTrust Signature Validation Vulnerability

CVE Number = CVE-2013-3900

QID: 90007 - Enabled Cached Logon Credential

CVE Number = None

QID: 78556 - Mozilla Firefox Multiple Vulnerabilities (MFSA2023-20)

CVE Number = CVE-2023-34414, CVE-2023-34415, CVE-2023-34417, CVE-2023-34416

QID: 378528 - Wireshark GDSDB dissector infinite loop Vulnerability (wnpa-sec-2023-14)

CVE Number = None

QID: Wireshark BLF file parser crash Vulnerability (wnpa-sec-2023-13)

CVE Number = CVE-2023-2857

QID: 78526 - Wireshark XRA dissector infinite loop Vulnerability (wnpa-sec-2023-20)

CVE Number = None

QID: Wireshark NetScaler file parser crash Vulnerability (wnpa-sec-2023-15)

CVE Number = CVE-2023-2858

QID: 378524 - Wireshark RTPS dissector crash Vulnerability (wnpa-sec-2023-18)

CVE Number = CVE-2023-0666

QID: Wireshark BLF file parser crash Vulnerability (wnpa-sec-2023-17)

CVE Number = CVE-2023-2854

QID: 378522 - Wireshark IEEE C37.118 Synchrophasor dissector crash Vulnerability (wnpa-sec-2023-19)

CVE Number = CVE-2023-0668

QID: 378521 - Wireshark VMS TCPIPtrace file parser crash Vulnerability (wnpa-sec-2023-16)

CVE Number = CVE-2023-2856

QID: 378520 - Wireshark Candump log file parser crash Vulnerability (wnpa-sec-2023-12)

CVE Number = CVE-2023-2855

Installation instructions: Reference the latest MSC upgrade documentation for the procedure.

<https://download.avaya.com/css/public/documents/101081871>

Avaya PDU Router (Linux):

Avaya PDU Router 5.0.0.7

This new PDU Router build 5.0.0.7 includes security fixes to multiple vulnerabilities identified on previous PDU Router versions up to **July 1st, 2023**. Any newer vulnerabilities

identified after cutover date will be addressed in the next release.

Vulnerabilities mitigated: RHSA-2023:3839, RHSA-2023:3840, RHSA-2023:3837, RHSA-2023:3827, RHSA-2023:3847, RHSA-2023:3425, RHSA-2023:3433, RHSA-2023:3349, RHSA-2023:2951, RHSA-2023:1566, RHSA-2023:0832.

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

HPE Nimble CS1000 Storage Array:

NimbleOS/Alletra Software Release 6.1.1.200-1020304

CVEs/Vulnerabilities mitigated: Critical fixes in this new release. See the release notes for more details.

[HPE Alletra 6000, Alletra 5000, HPE Nimble Storage Array OS 6.1.1.200 Release Notes](#)

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

Note: Array must be running NimbleOS 5.2.1.300 or later to update directly to NimbleOS 6.1.1.200.

Dell/EMC VNXe3200 Storage Array:

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

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.

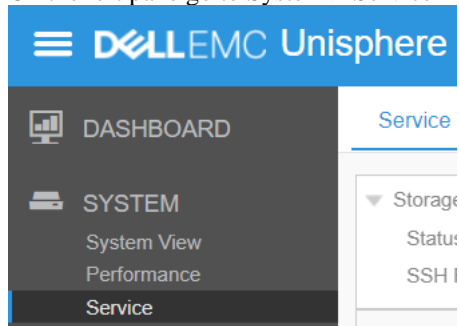
[VNXe3200-3.1.17.10229825-Release-Notes \(dell.com\)](#)

Upgrade instructions: See [PSN005974u](#) for the upgrade procedure.

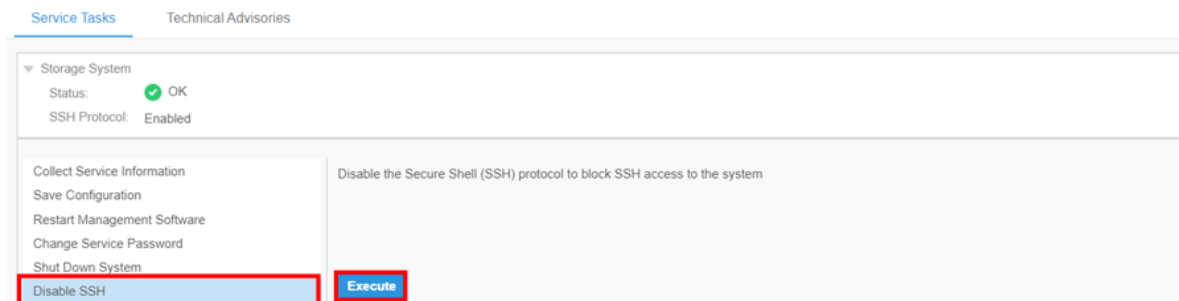
Workaround procedure to mitigate vulnerability CVE-2018-15473:

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.

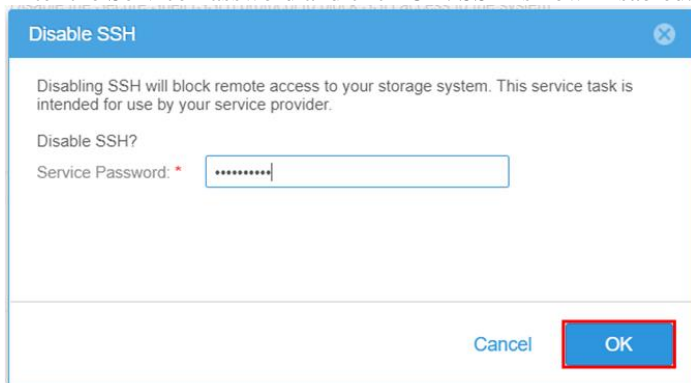
1. From the MSC, open a web browser to the IP/FQDN of the array and log in with the admin credentials. See the customer workbook for login details.
2. On the left pane go to System > Service



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



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



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.

All trademarks identified by ® or ™ are registered trademarks or trademarks, respectively, of Avaya LLC
All other trademarks are the property of their respective owners