Product Support Notice

PSN #	PSN005800u				
Original publication date: 18-Feb-2021. This is Issue #14, published date: 8-Nov-2022.	Severity/risk level	Medium	Urgency	When Convenient	

Name of problem

New Infrastructure Security Service Pack including ESXi, vCenter Server, Nimble, VNXe3200, Avaya Orchestrator, HPE Gen8/Gen9/Gen10 server, PDU, and VSP software and firmware available for ASP 4200 4.0/4.1/4.1.0.1 releases

Products affected

ASP 4200 4.x

Problem description

New Infrastructure Security Service Pack available for **ASP 4200 4.1** and **4.1.0.1** releases **only**. It includes the latest software and firmware approved by Avaya Engineering for ESXi 6.5, vCenter Server 6.5, Nimble CS1000, Dell/EMC VNXe3200, Avaya Orchestrator 1.5, VSP7254 and HPE Gen8/Gen9/Gen10 Servers. This Security Pack covers recently reported security vulnerabilities (CVEs) from the field as well as additional key fixes. The full Security Service Pack must be installed, with **no individual component upgrades.**

Resolution

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

UPDATE 11/08/2022

IMPORTANT: This is the last update being made available for the ASP 4200 4.x release. To continue support, upgrade to the ASP 4200 5.0 release.

New ZIP file: ASP4200_4.1.x_Infrastructure_Security_Service_Pack_Nov2022.zip
PLDS ID **CPOD0000224**

- New software and firmware available for several components in the solution. See the download section for the full list of new software and firmware files available. Some components do not have an updated release available at the time of this SSP update and are identified as “Same as with previous SSP” in the file list below. See the corresponding component sections below for further details.

UPDATE 03/15/2022

The updated version of the zip file - ASP4200_4.x_Infrastructure_Security_Service_Pack_v6_March2022.zip

- Support of vCenter 6.5 U3s Build 19261680
- Support of ESXi 6.5 EP26 Build 19092475

UPDATE 02/18/2022:

- Update to the “*HPE DL360 Gen9/Gen10v1/Gen10v2 Servers – Service Pack for ProLiant (SPP)*” section for observations and known issues. Issue observed on the Gen10v1/v2 servers after the SPP firmware package upgrade, the boot order may get changed. See the corresponding section below for more details and the workaround procedure.
- Added new information in the “*HPE DL360 Gen9/Gen10v1/Gen10v2 - Service Pack for ProLiant (SPP)*” section for firmware upgrade timing and recommendations.
- Added new important note to the “*QLogic 10Gb qfle3 driver update version 1.1.17.0”* section about unused NIC drivers.

UPDATE 02/07/2022:
HPE AMS driver correction for HPE Gen9/8 & Gen10 servers

Agentless Management Service (AMS)
Gen8-Gen9 AMS version **11.6.0-5**
Gen10 AMS version **11.8.0.15-1**

UPDATE 02/01/2022:
The updated version of the zip file - ASP4200_4.x_Infrastructure_Security_Service_Pack_v5_Feb2022.zip

- New sections added for the HPE Nimble CS1000 Storage Array and the HPE DL360 Gen8 Servers – Service Pack for ProLiant (SPP).
- New software and firmware available for several components in the solution. See the download section for the full list of new software and firmware files. See the corresponding component sections below for further details.

Avaya Orchestrator builds 47 is currently under testing and has not been finalized at the time of publishing this update to the PSN. The new AO build will be released at a future date.

UPDATE 11/22/2021:
The updated version of the zip file - ASP4200_4.x_Infrastructure_Security_Service_Pack_v4_Nov2021.zip

- New section added for the Dell/EMC VNXe3200 Storage array.
- New software release v3.1.15 available for installation and upgrade on the VNXe3200 Storage array. SSH disablement procedure added to mitigate CVE-2018-15473 (OpenSSH).
- Added VSP7254 VOSS 8.1.10 software to the SSP .zip file bundle.

UPDATE 10/08/2021:
- Upgrade considerations for ASP4200 4.0 customers added to the Patch installation section.
- Updated FW version for the VSP 7254 switches.

UPDATE 10/04/2021: Updated version of the zip file – ASP4200_4.x_Infrastructure_Security_Service_Pack_v3_Oct2021.zip to include updated vCenter and ESXi patches. See the *VMware* section for more details. No other changes to the firmware/software in the .zip file.

UPDATE 08/09/2021: Update to the "*QLogic 10Gb qfle3 driver update version 1.1.12.0*" section to include important information on procedures that must be confirmed and conducted before the driver is updated.

UPDATE 06/14/2021: Updated version of the zip file - ASP4200_4.x_Infrastructure_Security_Service_Pack_v2_June2021.zip to include updated vCenter and ESXi patches, 10Gb qfle3 NIC driver as well as a new SPP .iso image to include latest BIOS/iLO/Storage Controller/1GB-10GB NIC firmware.

UPDATE 04/28/2021: Informational VIB files description added pertain to ESXi650-202011002.zip (updated for *ESXi650-202102001.zip* on 6/2021*)*. This is needed when creating and updating the vSphere Update Manager repository and software baselines. There are no software changes with this update. See the VMware section down below for further information.

UPDATE 04/19/2021: Adding to Infrastructure Security Service Pack new Avaya Orchestrator 1.5 build 46.

UPDATE 03/2021: Adding support for the Security Service Pack to be installed on ASP 4200 4.0 releases.

Workaround or alternative remediation

n/a

Remarks

n/a

Procedures

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

Backup before conducting procedures

n/a

Download

PLDS ID **CPOD0000224** – ASP4200_4.1.x_Infrastructure_Security_Service_Pack_Nov2022.zip

Upgrade FW/SW files included in new ZIP file:

- ***New*** HPE-Alletra-6.0.0.500-1005932-opt.update.v2
- ***New*** 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)
- ***New*** pro-v80x.bin
- ***New*** bp-avaya-dl360g8-ASP4200-4-1-0-1-B5-Legacy-only.iso
- ***New*** bp-avaya-dl360g9-ASP4200-4-1-0-1-B6.iso
- ***New*** bp-avaya-dl360g10-ASP4200-4-1-0-1-B6.iso
- ***New*** ESXi650-202210001.zip
- ***New*** VMware-vCenter-Server-Appliance-6.5.0.41000-20510539-patch-FP.iso
- ***New*** ams-esxi6.5-bundle-gen9.11.8.0.5-1.zip
- ***New*** VOSS4K.7.1.11.0.tgz
- ***New*** VOSS7400.8.8.0.0.tgz
- VMW-ESX-6.5.0-nhpsa-65.0072.0.149-offline_bundle-17204132.zip ➔ Vendor latest driver (**Same as with the previous SSP**)
- ams-esxi6.5-bundle-gen10.11.8.0.15-1.zip ➔ Vendor latest driver (**Same as with the previous SSP**)
- ams-esxi6.5-bundle-11.6.0-5.zip ➔ Vendor latest driver (**Same as with the previous SSP**)
- VMW-ESX-6.5.0-smartpqi-65.4150.0.119-offline_bundle-18379836.zip ➔ Vendor latest driver (**Same as with the previous SSP**)
- MRVL-E3-Ethernet-iSCSI-FCoE-1.0.143-offline_bundle-18284876.zip ➔ Vendor latest driver (**Same as with the previous SSP**)
- VOSS7200.8.1.10.0.tgz ➔ Vendor latest FW (**Same as with the previous SSP**)
- smcdu-v71f.bin ➔ Vendor latest FW (**Same as with the previous SSP**)
- swcdu-v71f.bin ➔ Vendor latest FW (**Same as with the previous SSP**)

Avaya Orchestrator:

Note: Customers currently running AO build **47** can skip. Perform upgrade activity once AO builds 50 becomes available instead.

- AvayaOrchestrator_1.5.0.0.22052347_vmx.ova- PLDS ID: **CPOD0000240**
- avayaorchestrator.1.5.0.047.iso- PLDS ID: **CPOD0000241**

Patch Installation Instructions	Service-interrupting?
	Yes

Important:
The following software and firmware are available to be applied on ASP 4200 4.1 and 4.1.0.1 environments **only**. The full Security Service Pack must be installed, with **no individual component upgrades**.

A step-up upgrade to release **4.1.0.1** is required for customers with 4200 racks running at release **4.0** before applying the **November 2022 SSP**. **DO NOT** upgrade ESXi hosts directly from the ASP 4200 4.0 release (ESXi 6.5 U2) to ESXi650-202210001 (ESXi 6.5 P09) as relevant VIBs to HPE servers released in the HPE custom image for ESXi U3 will be missed, thus potentially leaving servers in an unsupported state.

Prerequisites:

- Overall health of the infrastructure components is in a healthy state. All alarms should be resolved before scheduling 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 the documentation of each application.
- Use the workflow below when planning the maintenance activities.
- Download the corresponding ZIP file from PLDS and place it on the MSC.

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

New with SPP iso images:

- Gen9 SPP file: bp-avaya-dl360g9-ASP4200-4-1-0-1-B6.iso
- Gen10v1/v2 SPP file: bp-avaya-dl360g10-ASP4200-4-1-0-1-B6.iso
  Installation instructions: Reference the latest MSC upgrade documentation for the procedure. https://downloads.avaya.com/css/P8/documents/101070494
- The network connectivity issue when upgrading server FW using the iLO shared feature is fixed.
- Server upgrades may now be conducted remotely without the need of burning a DVD with the HPE SPP ISO image, however, based on the extended time it takes to conduct the firmware upgrade remotely (which **can take up to or beyond 2 hours per server**) it is recommended to dispatch a tech onsite to burn the SPP ISO image and run the upgrade with the DVD. This is the recommended method if several hosts require an upgrade, and a limited maintenance window is provided. The extended time to conduct the firmware upgrade is due to a performance bottleneck in the Windows Server 2016 MSC. In the ASP4200 5.0 release, this issue is fixed as the new MSC is Windows Server 2019.
- iLO FW continues to be included with the SPP as a result of the network connectivity fix.

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

Contents of HPE Gen10v1/v2 SPP image:

Name	Version	CVEs mitigated / Bug fixes
HPE Integrated Lights-Out 5	2.72	No vulnerabilities. Includes enhancements and 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	2.29.2 (HPE v7.18.82) MFW 7.16.03	No vulnerabilities. Includes bug fixes.
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)	No vulnerabilities. Includes enhancements and bug fixes.
HPE ProLiant DL360 Gen10 (U32) Server BIOS	2.68_2022_07_14	CVE-2022-2068, CVE-2022-27404, CVE-2022-27405, CVE-2022-27406. Includes enhancements and bug fixes.

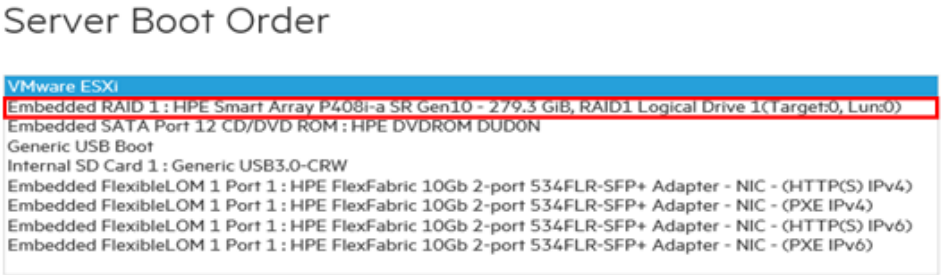
Contents of HPE Gen9 SPP image:

Name	Version	CVEs mitigated / Bug fixes
HPE Integrated Lights-Out 4	2.81	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	2.29.2 (HPE v7.18.82) MFW 7.16.03	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	7.00	No vulnerabilities. Includes enhancements and bug fixes.
HPE ProLiant DL360 Gen9 (P89) Server BIOS	3.02_2022_07_18	No vulnerabilities. Includes bug fixes.

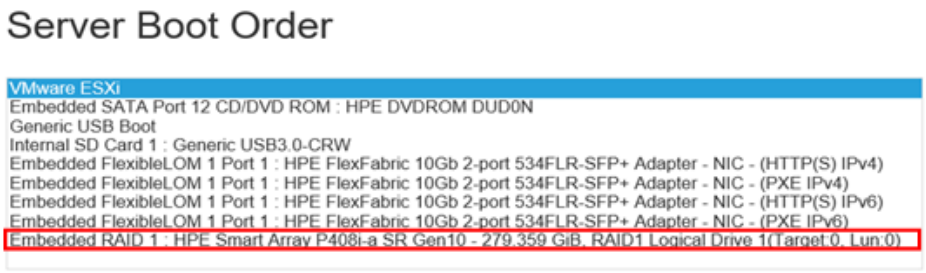
Observations and known issues:

- 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.

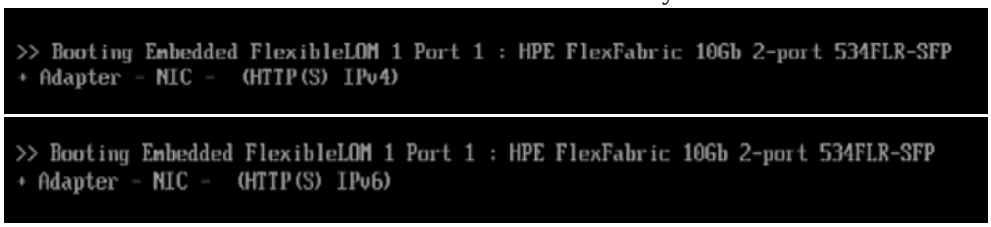
  Server boot order before firmware upgrade:
  Embedded RAID 1: HPE Smart Array is second from the top in the boot order.



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



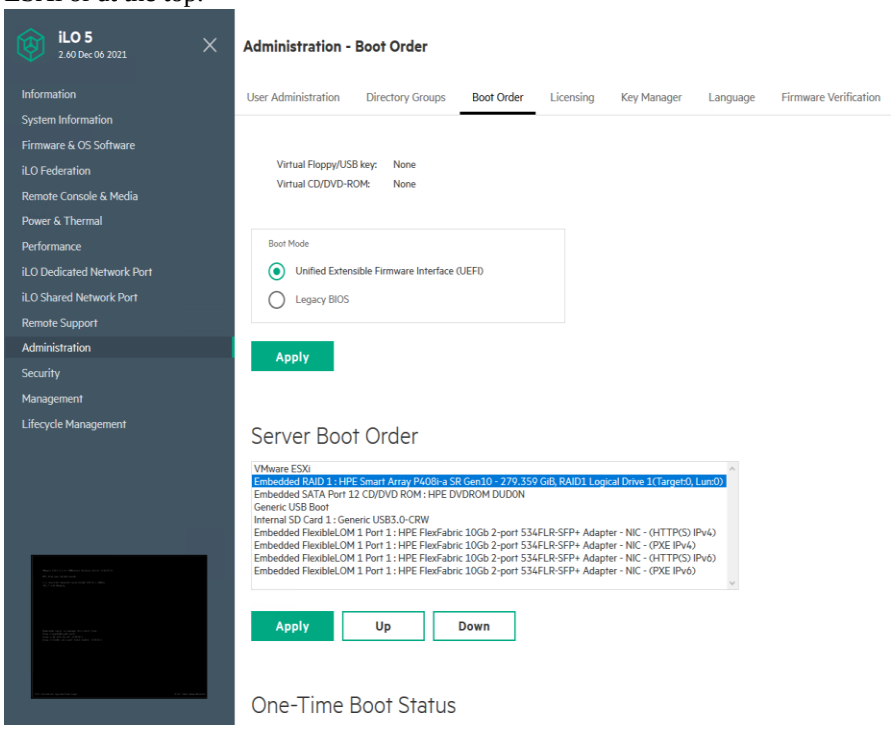
When the server reboots, it tries to boot from the NICs first before booting from the ESXi OS located on the Embedded RAID 1: HPE Smart Array :



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.

HPE DL360 Gen8 Servers – Service Pack for ProLiant (SPP):

New SPP iso image: bp-avaya-dl360g8-ASP4200-4-1-0-1-B5-Legacy-only.iso
Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://downloads.avaya.com/css/P8/documents/101070494

Contents of SPP image:

Name	Version	CVE's / Fixes
HPE Integrated Lights-Out 4	2.81	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	2.29.2 (HPE v7.18.82) MFW 7.16.03	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	7.00	No vulnerabilities. Includes enhancements and bug fixes.
HPE Smart Array P220i, P222, P420i, P420, P421, P721m, and P822	8.32	No vulnerabilities. Includes bug fixes.
HPE Smart Array P230i, P430, P431, P731m, P830i, and P830	5.02	No vulnerabilities. Includes bug fixes.
HPE ProLiant DL360p Gen8 (P71) Server BIOS	2019.05.24	CVE-2018-12126, CVE-2018-12130, CVE-2018-12127 and CVE-2019-11091
HPE ProLiant DL360e Gen8 (U73) Server BIOS	2019.05.24	CVE-2018-12126, CVE-2018-12130, CVE-2018-12127 and CVE-2019-11091

VMware:

VMware vCenter Server 6.5 U3u build 20510539
CVEs/Vulnerabilities mitigated: CVE-2022-31680, VMSA-2022-0025

https://docs.vmware.com/en/VMware-vSphere/6.5/rn/vsphere-vcenter-server-65u3u-release-notes.html

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

VMware ESXi 6.5 P09 build 20502893
CVEs/Vulnerabilities mitigated: CVE-2022-31681, CVE-2018-5733, VMSA-2022-

0025

Note: The roll-up bulletins contain the latest VIBs with all the fixes since the initial release of ESXi 6.5.

https://docs.vmware.com/en/VMware-vSphere/6.5/rn/esxi650-202210001.html

vSphere Update Manager information:

Name	ID	ESXi Version	Severity	Category	Release Date	Type	Vendor
VMware ESXi 6.5 Patch Release	ESXi650-202210001	6.5.0	Important	BugFix	10/5/2022, 8:00 PM	Rollup	VMware, Inc
Updates esx-base, esx-tboot, vsan and vsanhealth VIBs	ESXi650-202210101-SG	6.5.0	Important	Security	10/5/2022, 8:00 PM	Patch	VMware, Inc
Updates tools-light VIB	ESXi650-202210102-SG	6.5.0	Important	Security	10/5/2022, 8:00 PM	Patch	VMware, Inc
Updates esx-base, esx-tboot, vsan and vsanhealth VIBs	ESXi650-202210401-BG	6.5.0	Important	BugFix	10/5/2022, 8:00 PM	Patch	VMware, Inc
Updates ntg3 VIB	ESXi650-202210402-BG	6.5.0	Important	BugFix	10/5/2022, 8:00 PM	Patch	VMware, Inc

Rollup Bulletin

Bulletin ID	Category	Severity
ESXi650-202210001	Bugfix	Important

Bulletins

Bulletin ID	Category	Severity
ESXi650-202210101-SG	Security	Important
ESXi650-202210102-SG	Security	Important
ESXi650-202210401-BG	Bugfix	Important
ESXi650-202210402-BG	Bugfix	Important

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

Qlogic, AMS, and Storage Controller Drivers:

QLogic 10Gb qfle3 driver update version 1.1.17.0 (Same as with the previous SSP)

STOP! - IMPORTANT: Before beginning the qfle3 driver update to the latest version 1.1.17.0 below, **confirm that the unused qfle3i, qfle3f, and qcnic drivers are not enabled on the host**. Failure in doing so creates a conflict with the iSCSI Network Port Binding settings on the ESXi host. See the latest MSC upgrade document for the procedures to disable these drivers: https://downloads.avaya.com/css/P8/documents/101070494 procedures on pg.81-84.

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

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

MFW/Firmware: *7.16.3*
Driver Version: *1.1.17.0*

```
[root@cpd6-esxi3:~] esxcli network nic get -n vmnic4
   Advertised Auto Negotiation: false
   Advertised Link Modes: 10000BaseTwinax/Full
   Auto Negotiation: false
   Cable Type: DA
   Current Message Level: 0
   Driver Info:
         Bus Info: 0000:04:00:0
         Driver: qfle3
         Firmware Version: Storm: 7.13.18.1 MFW: 7.16.3
         Version: 1.1.17.0
   Link Detected: true
   Link Status: Up
   Name: vmnic4
   PHYAddress: 0
   Pause Autonegotiate: false
   Pause RX: true
   Pause TX: true
   Supported Ports: FIBRE
   Supports Auto Negotiation: false
   Supports Pause: true
   Supports Wakeon: true
   Transceiver: external
   Virtual Address: 00:50:56:17:88:60
   Wakeon: MagicPacket(tm)
```

Agentless Management Service (AMS)

Gen8 AMS version 11.6.0-5 (**Same as with the previous SSP**)
Gen9 AMS version 11.8.0.5-1
Gen10 AMS version 11.8.0.15-1 (**Same as with the previous SSP**)
Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://downloads.avaya.com/css/P8/documents/101070494

Storage Controller (Same as with the previous SSP)

Gen8 and Gen9 Storage Controller version 65.0072.0.149
Gen10 Storage Controller version 65.4150.0.119
Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://downloads.avaya.com/css/P8/documents/101070494

Avaya Orchestrator 1.5

Pending: Avaya Orchestrator build 50 is currently under development and has not been finalized at the time of publishing this update to the PSN. The new AO build will be released at a future date.

Note: Customers currently running AO build **47** can skip. Perform upgrade activity once AO builds 50 becomes available instead.

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 8.8.0.0
CVEs/Vulnerabilities mitigated: This switch firmware includes several resolved issues, incorporating all fixes from prior releases.
Installation instructions: Reference the latest MSC upgrade documentation for the procedure. The procedure is the same for the 7400 switches as the 7254's.
https://downloads.avaya.com/css/P8/documents/101070494

VSP4850 network switches VOSS 7.1.11.0
CVEs/Vulnerabilities mitigated: This switch firmware includes several resolved issues, incorporating all fixes from prior releases.
Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://downloads.avaya.com/css/P8/documents/101070494

VSP7254 network switches VOSS 8.1.10.0 (Same as with the previous SSP)
CVEs/Vulnerabilities mitigated: This switch firmware includes several resolved issues, incorporating all fixes from prior releases. High-priority software defect fix included which has been seen in previous releases of VOSS in earlier releases of PodFx: "*GlobalRouter MLT WARNING 29781608 uSecs elapsed since smltTick last ran. tMAIN latency is HIGH !*"
Installation instructions: Reference to PSN005904u.

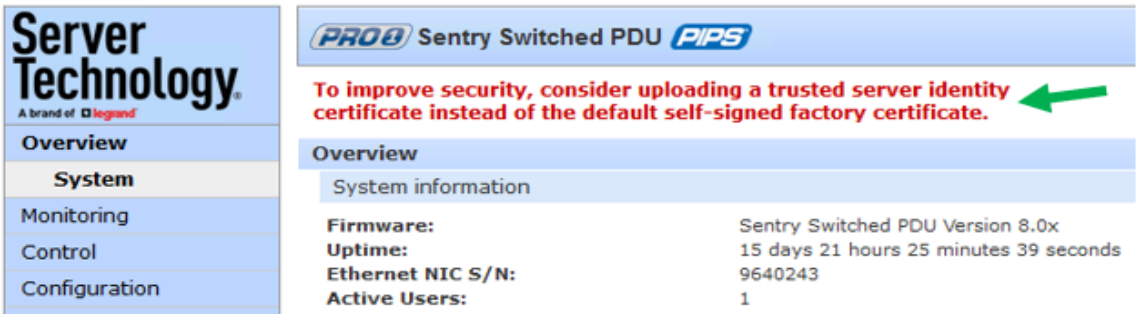
PDUs:

Sentry3 PDU (Smart & Switched) version v71f (Same as with previous SSP)
CVEs/Vulnerabilities mitigated: This PDU firmware version removed MS SYNC from the Treck TCP/IP stack to stop security scanners from giving a false positive for Ripple20 vulnerabilities.
Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://downloads.avaya.com/css/P8/documents/101070494

Sentry4 PDU version v80x
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://downloads.avaya.com/css/P8/documents/101070494

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.



HPE Nimble CS1000 Storage Array:

NimbleOS/Alletra Software Release 6.0.0.500-1005932
CVEs/Vulnerabilities mitigated: Several critical fixes in this new release. See the release notes for more details.
HPE Alletra 6000, HPE Nimble Storage Array OS 6.0.0.500 Release Notes
Installation instructions: Reference the latest MSC upgrade documentation for the procedure.
https://downloads.avaya.com/css/P8/documents/101070494

Note: Array must be running NimbleOS 5.0.6.0 or later to update directly to NimbleOS 6.0.0.500.

Dell/EMC VNXe3200 Storage Array:

Software Release v3.1.17.10229825

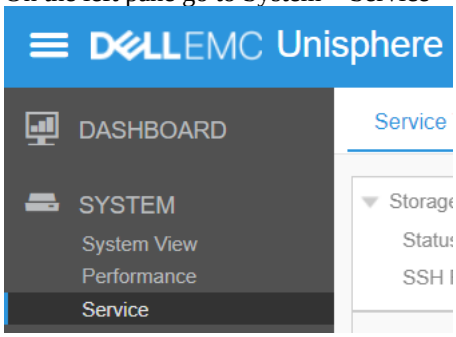
Important:
Please note that this is v3.1.17 but it's a different build number than the previous release (3.1.17.**10223906**)

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.

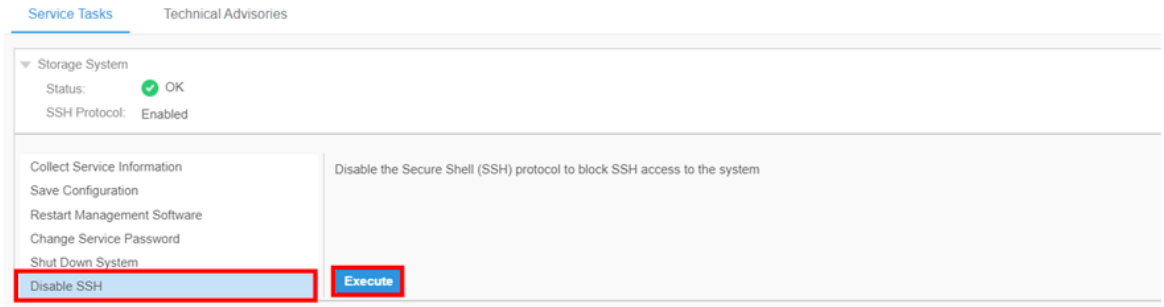
Workaround procedure to mitigate vulnerability CVE-2018-15473:

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.

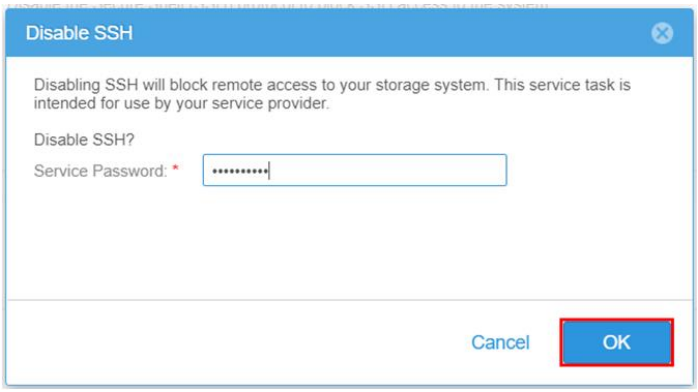
1. From the MSC, open a web browser to the IP/FQDN of the array and log in with the admin credentials. See the customer workbook for login details.
2. On the left pane go to System > Service



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.

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.