Product Support Notice

PSN #	PSN005974u	Avaya Proprietary – Use pursuant to the terms of your signed agreement or company policy.

Original publication date: 17-Dec-21. This is issue #05, published date 14-Jan-22.	Severity/risk level	High	Urgency	Immediately

Name of problem	PSN005974u – ACP 4200/ASP 4200 Log4j

Products affected

Avaya Converged Platform 4200 4.0, Avaya Solutions Platform 4200 4.0, Avaya Solutions Platform 4200 4.1.x

Problem description

Avaya is aware of the recently identified Apache Log4j vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832, CVE-2021-4104) and is conducting impact assessments across its portfolio, identifying opportunities for temporary mitigations, if possible, and developing plans for remediation. Reference the *Avaya Product Security - **Apache Log4j Vulnerability - Impact for Avaya products*** on support.avaya.com for updates

ACP 4200/ASP 4200 Releases and Impacts:

Avaya Converged Platform 4200 4.0, Avaya Solutions Platform 4200 4.0, Avaya Solutions Platform 4200 4.1.x – Impact assesment by CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104 and CVE-2021-44832.

Individual component impact:

❖ VMware vCenter Server **6.5.x**

- **CVE-2021-44228 & CVE-2021-45046**: Impacted. Workaround available and patch is still pending at the time of publising this article. Avaya has completed testing and validating the provided workaround by the vendor. Customers may now proceed with implementing workaround at the earliest convenience. Reference to the workaround section in this PSN for details and instructions.
- **CVE-2021-45105 and CVE-2021-44832:** At the time of publishing this article, VMWare has not found a valid attack vector to exploit CVE-2021-45105 in any VMware products, but investigations will continue. VMware will update in their products log4j to 2.17 in future releases.
  Reference to VMSA-2021-0028.8 for further information.
- **CVE-2021-4104:** At the time of publishing this article the vendor has not released information regards to CVE-2021-4104 in their security advisory VMSA-2021-0028.8. Avaya will continue updating this PSN as updates become publicly available by the vendor.

❖ VMware ESXi 6.5.x

- **CVE-2021-44228 & CVE-2021-45105:** Not impacted
  Reference to KB Article 87068 for further information.
- **CVE-2021-45046, CVE-2021-44832 & CVE-2021-4104:** Not impacted.
  Reference to KB Article 87068 & VMSA-2021-0028.8 for further information.

❖ Extreme VSP 7024 Network Switches

- **CVE-2021-44228 :** The BOSS OS running on the data switches is not impacted by CVE-2021-44228.
- **CVE-2021-45046, CVE-2021-45105 , CVE-2021-44832 & CVE-2021-4104:** The OS running on the data switches is not impacted by CVE-2021-44228 therefore is not impacted by current and future subsets of the Log4j vulnerability.
  Reference to VN-2021-465 for further information.

❖ Extreme VSP 4850 Network Switches

- **CVE-2021-44228 :** The VOSS OS running on the data switches is not impacted by CVE-2021-44228.

- **CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104:** The OS running on the data switches is not impacted by CVE-2021-44228 therefore is not impacted by current and future subsets of the Log4j vulnerability.
  Reference to VN-2021-465 for further information.

❖ Extreme VSP 7254 Network Switches

- **CVE-2021-44228 :** The VOSS OS running on the data switches is not impacted by CVE-2021-44228.
- **CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104:** The OS running on the data switches is not impacted by CVE-2021-44228 therefore is not impacted by current and future subsets of the Log4j vulnerability.
  Reference to VN-2021-465 for further information.

❖ Dell/EMC VNXe3200 Storage Array

- **CVE-2021-44228 & CVE-2021-45046:** Impacted. New firmware has been released by the vendor; however, it uses Log4j 2.16.
  Reference to Dell Security Article 000194414 & DSA-2021-298 for further reference.
  Avaya has completed testing and validating the new fimware released by the vendor. Customers may now proceed with upgrading the SAN at the earliest convenience. Reference to the resoluton section in this PSN for FW details and instructions.
- **CVE-2021-45105, CVE-2021-44832:** At the time of publishing this article vendor is not aware of attackers exploting CVE-2021-45105 and will continue to monitor the impact and any other issues discovered that may accelerate remedy timelines if cirmcustances change.
  Reference to Dell Security Article 000194416 for further reference.
- **CVE-2021-4104:** At the time of publishing this article the vendor has not released information regards to CVE-2021-4104 to Security Articles 000194416 or 000194372 both tracking Dell Response to Apache Log4j Code Execution. Avaya will continue updating this PSN as updates become publicly available by the vendor. However, Avaya recommends upgrading to FW 3.1.17.10223906 to protect against CVE-2021-44228 and subsequently CVE-2021-45046.

❖ HPE/Nimble CS1000 Storage Array

- **CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104 & CVE-2021-44832:** Not Impacted.
  Reference to Customer Notice a00120086 for further information.

❖ HPE DL360 Gen8 Servers / iLO4

- **CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104 & CVE-2021-44832:** Not Impacted.
  Reference to Customer Notice a00120086 for further information.

❖ HPE DL360 Gen9 Servers / iLO4

- **CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104 & CVE-2021-44832:** Not Impacted.
  Reference to Customer Notice a00120086 for further information.

❖ HPE DL360 Gen10 v1 and v2 Servers / iLO5

- **CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104 & CVE-2021-44832:** Not Impacted.
  Reference to Customer Notice a00120086 for further information.

❖ Sentry 3 & 4 PDUs

- **CVE-2021-44228 :** The firmware running on the PDUs is not impacted by CVE-2021-44228.
- **CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104:** The firmware running on the PDUs is not impacted by CVE-2021-44228 therefore is not impacted by current and future subsets of the Log4j vulnerability.
  Reference to https://www.servertech.com/support for further information.

❖ Avaya Orchestrator 1.5

- **CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104:** Not impacted. As confirmed by our vendor, the Apache versions used in Nagios XI are not vulnerable to the Log4j vulnerabilities. AO uses Nagios XI 5.5.9-2
  Reference to https://www.nagios.com/news/2021/12/update-on-apache-log4j-vulnerability/ for further information.

❖ Management Server Console (MSC)

- **CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104:** Not impacted. The Windows Server 2016 OS that comes with the MSC OVA does not have any JAVA based application pre-installed.

❖ PDU Router

- **CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104:** Not impacted. The Windows Server 2016 OS that comes with the MSC OVA does not have any JAVA based application pre-installed.

Please only follow documented procedures described in this PSN to resolve this issue.

This PSN will be updated as more information is available.
Ensure that you are signed up for Avaya E-notifications so that you will be notified when new issues of this PSN are posted.

Resolution

- Dell/EMC VNXe3200 Storage Array release v3.1.17.10223906 mitigates Log4j vulnerability CVE-2021-44228: DSA-2021-298. See the Patch install instructions section below for the upgrade procedure. See the Download section for the PLDS ID for the new release file.

Workaround or alternative remediation

Workaround instructions to address CVE-2021-44228 and CVE-2021-45046 in vCenter Server

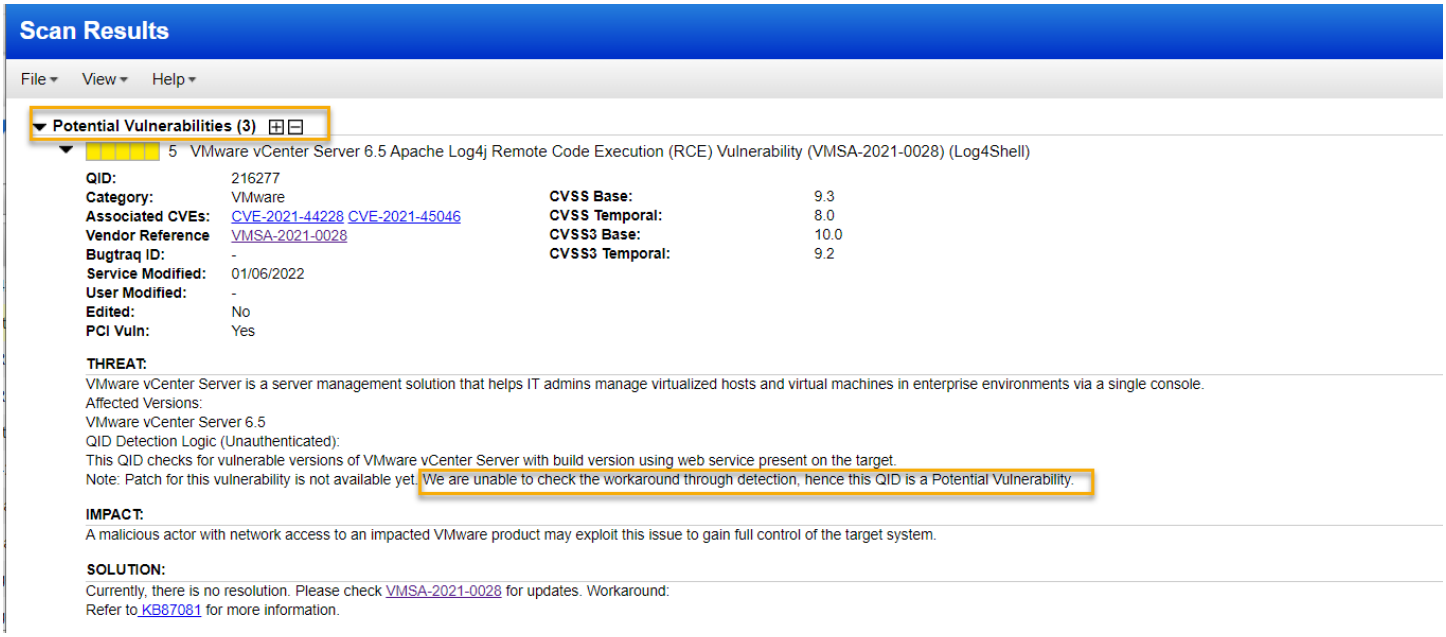
Purpose

The workarounds described in this document are meant to be a temporary solution only. Reference to KB 87081 for further information.

Note:

This is a service affecting activity. vCenter will be inaccessible throughout this process therefore conduct mitigation activity during a customer approved maintenance activity.

Note: Vulnerability scan results may still detect or discover CVE-2021-44228, CVE-2021-4506 in vCenter after implementing the workaround. This is a limitation with the scanner as it is unable to check or detect the workaround through detection, hence flagging vulnerabilities.



Procedure

1) Download from PLDS the workaround script "`vc_log4j_mitigator.py`" and transfer the file to the Management Server Console.
2) Login to the vCSA using an SSH Client (using Putty.exe available with the MSC VM)
3) Transfer the file to /tmp folder on vCenter Server Appliance using WinSCP
   Note: It's necessary to enable the bash shell before WinSCP will work
4) Execute the script copied in step 1:

```
python vc_log4j_mitigator.py
```

This will stop all vCenter services, updates all necessary files with the formatMsgNoLookups flag, removes the JndiLookup.class from all jar/war files on the appliance, and finally starts all vCenter services. The files that the script modifies will be reported as the script runs.

```
root@mainpod-vcenter [ ~ ]# cd /tmp/
root@mainpod-vcenter [ /tmp ]# ls
deploy.vib._nrt_a           hsperfdata_eam         hsperfdata_vapiEndpoint    jna-content-library
eam5813741014644304397      hsperfdata_perfcharts  hsperfdata_vsan-health     jna-root
eam7840461185353001234      hsperfdata_root        hsperfdata_vsphere-client  vc_log4j_mitigator.py
hsperfdata_content-library  hsperfdata_updatemgr   hsperfdata_vsphere-ui      vmware-root_1440-2689143941
root@mainpod-vcenter [ /tmp ]#
root@mainpod-vcenter [ /tmp ]#
root@mainpod-vcenter [ /tmp ]# python vc_log4j_mitigator.py
2021-12-22T12:37:30 INFO main: Script version: 1.6.0
2021-12-22T12:37:30 INFO main: vCenter type: Version: 6.5.0.37000; Build: 18499837; Deployment type: embedded; Gateway: False; VCHA: False;
 Windows: False;
A service stop and start is required to complete this operation.  Continue?[y]y
2021-12-22T12:37:47 INFO stop: stopping services
```

```
/usr/lib/vmware-sso/vmware-sts/webapps/sts.war
/usr/lib/vmware-sso/vmware-sts/webapps/websso.war
/usr/lib/vmware-sso/vmware-sts/webapps/idm.war
/usr/lib/vmware/common-jars/log4j-core-2.11.2.jar
/usr/lib/vmware-cm/lib/log4j-core.jar
/opt/vmware/lib64/log4j-core-2.11.2.jar

List of processed configuration files:

/usr/lib/vmware-vmon/java-wrapper-vmon
/etc/rc.d/init.d/vmware-psc-client
/etc/rc.d/init.d/vmware-stsd
/etc/rc.d/init.d/vmware-sts-idmd

Total fixed: 14

    NOTE: Running this script again with the --dryrun
    flag should now yield 0 vulnerable files.  <----

Log file: /var/log/vmsa-2021-0028_2022_01_05_17_03_49.log
==========================
2022-01-05T10:06:23 INFO start: starting services
2022-01-05T10:09:31 INFO main: Done.
root@mainpod-vcenter [ /tmp ]#
```

5) To verify that no more vulnerable files exist, execute the script again with the dry run flag:

   `python vc_log4j_mitigator.py -r`

   The list of vulnerable files should be zero

```
root@mainpod-vcenter [ /tmp ]# python vc_log4j_mitigator.py -r
2022-01-05T10:18:01 INFO main: Script version: 1.6.0
2022-01-05T10:18:01 INFO main: vCenter type: Version: 6.5.0.38000; Build: 18711281; Deployment type: embedded; Gateway: False; VCHA: False; Windows: Fal
se;
2022-01-05T10:18:01 INFO main: Running in dryrun mode.
2022-01-05T10:18:24 INFO print_summary:
=====     Summary     =====

No vulnerable files found!

Total found: 0
Log file: /var/log/vmsa-2021-0028_2022_01_05_17_18_01.log
==========================
2022-01-05T10:18:24 INFO main: Done.
root@mainpod-vcenter [ /tmp ]#
```

Remarks

PSN Revision History
Issue 1 – December 17, 2021: Initial publication.
Issue 2 – December 21, 2021: Problem description updated.
Issue 3 – December 28, 2021: Update to Avaya Orchestrator 1.5.
Issue 4 – January 5, 2022 : Update to cover CVE-2021-44832 & CVE-2021-4104, vCenter workaround, new FW for VNXe3200.
Issue 5 – January 14, 2022: Update to vCenter, Nimble and server/iLO items for CVE-2021-44832. New warning note for the VNXe3200 upgrade procedure.

Patch Notes

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

Backup before applying the patch

Always

Download	
Dell/EMC VNXe3200: PLDS ID# **CPOD0000220** VMware vCenter Server Appliance: PLDS ID# **CPOD0000221**	
Patch install instructions	Service-interrupting?
Dell/EMC VNXe3200 Storage Array upgrade to v3.1.17:	Yes

Software Release v3.1.17.10223906

Upgrade instructions:

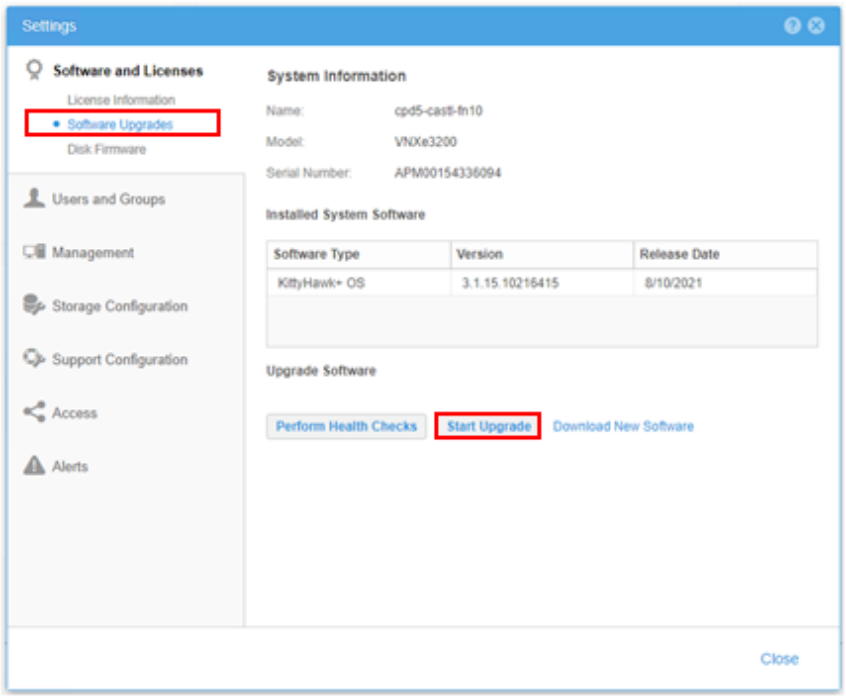
Important: Confirm that the storage array is in a healthy state and that there are no existing alarms or issues reported (**faulted SPs, batteries, hard drives, network ports down, etc**), any issues must be fixed prior to attempting the upgrade activity.

Warning: Confirm that there are multipath/redundant connections from the Storage array to the ESXi hosts in the environment prior to starting the upgrade activity. Failure to validate redundancy can severely impact the overall solution.

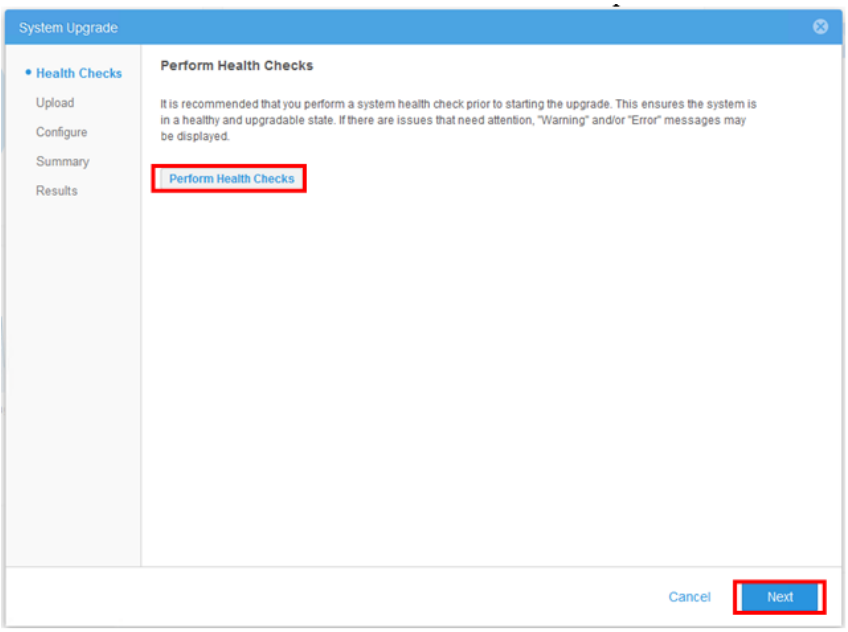
Note: Copy the VNXe-3.1.17.10223906.tgz.bin.gpg file to the Management Server Console (MSC) before beginning the upgrade procedure.

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. At the top-right side of the GUI, select the gear shaped icon to open the settings menu.

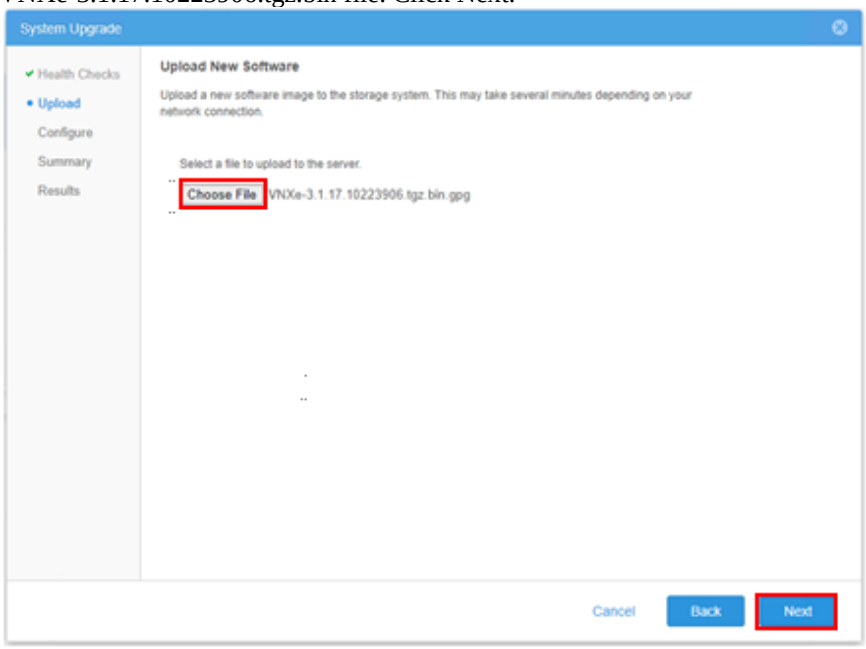
3. From the settings menu go to Software and Licenses > Software Upgrades



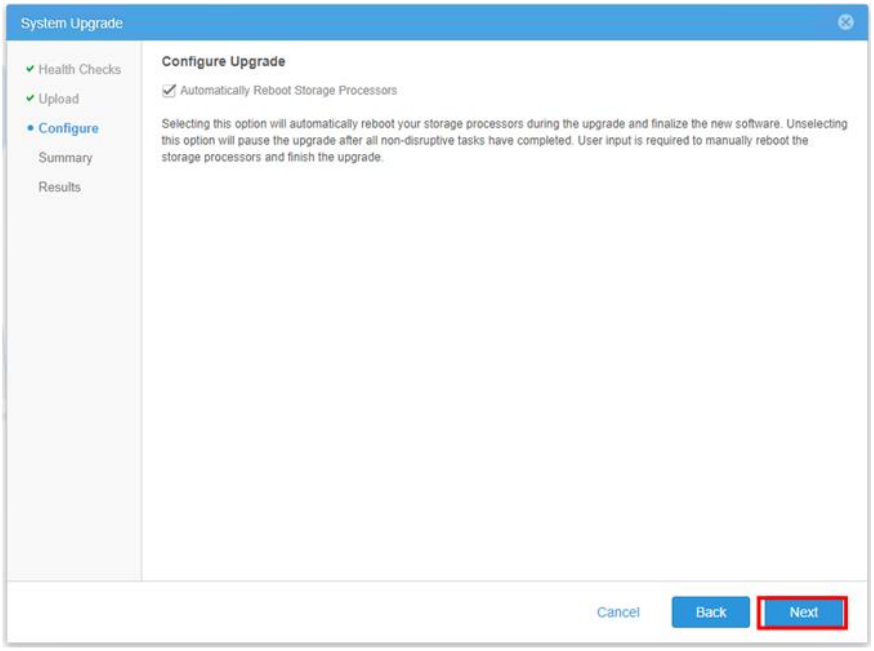
4. Under Upgrade Software select Start Upgrade
5. Click Perform Heath Checks. Once the health check completes click Next.



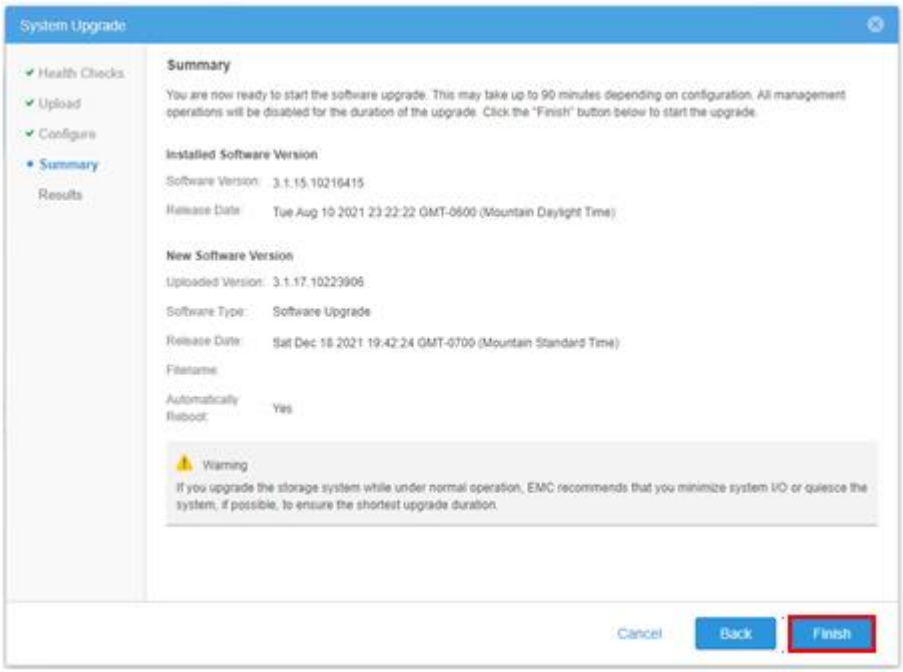
6. Upload the new software by clicking “Choose File” and going to and selecting the VNXe-3.1.17.10223906.tgz.bin file. Click Next.



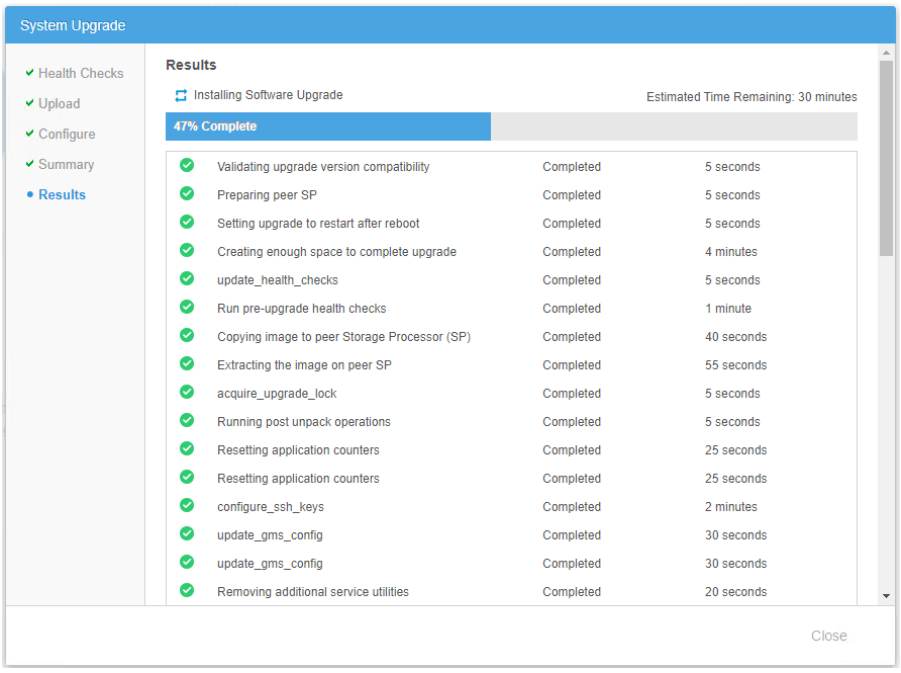
7. For the Configure Upgrade tab, leave as defaults, and click Next.



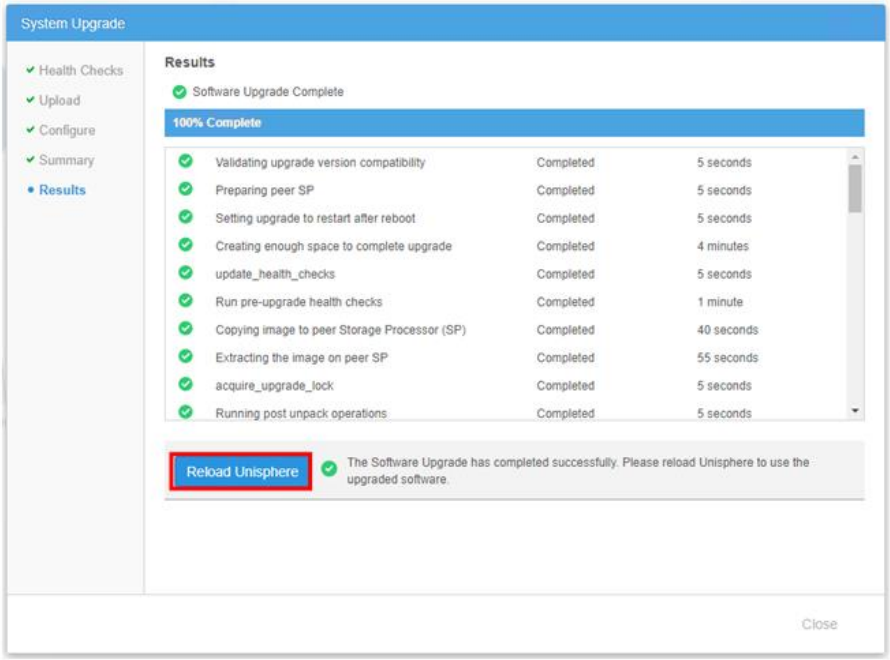
8. Summary is provided to display the currently installed software and the new software that is to be installed. Click Finish to start the upgrade.



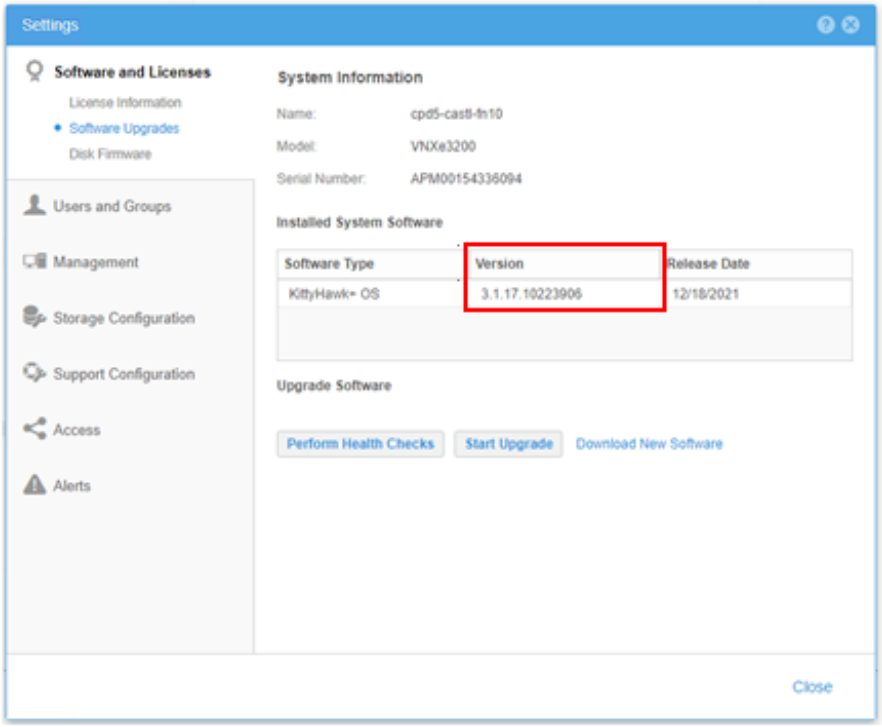
9. Window is displayed showing the software is being upgraded.



10. Once the upgrade completes, select “Reload Unisphere” to load Unisphere using the new upgraded software.



11. To confirm the upgrade and version installed, go to the gear shaped icon at the top-right and view the version under Software and Licenses > Software Upgrades > Installed System Software.



Verification

Reference to Patch installation and workaround section.

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

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

Security risks

Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45105
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104

Reference https://logging.apache.org/log4j/2.x/security.html

Avaya Security Vulnerability Classification

Reference www.avaya.com/emergencyupdate

Mitigation

As noted in this PSN.

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 INC., 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.