

Product Support Notice

© 2021 Avaya Inc. All Rights Reserved.

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 #08, published date Severity/risk level High Urgency Immediately 22-Feb-22.

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 (<u>CVE-2021-44228</u>, <u>CVE-2021-45046</u>, <u>CVE-2021-45046</u>, <u>CVE-2021-45046</u>, <u>CVE-2021-44832</u>, <u>CVE-2021-44832</u>, <u>CVE-2021-4104</u>) 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* - <u>Apache Log4j Vulnerability - Impact for Avaya products</u> 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 assessment 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
 - <u>CVE-2021-44228 & CVE-2021-45046</u>: Impacted. VMware has released vCenter Server Appliance 6.5 U3s- Build 19261680 which updates <u>apache log4j</u> to versions <u>2.12.4 for JDK 7 and 2.17.0 for JDK 8</u> to resolve CVE-2021-44228 and CVE-2021-45046. Avaya has concluded the testing and validation of the new updated VCSA version and customers may now proceed with updating the vCenter Server Appliance to release 6.5 U3s- Build 19261680 at the earliest convenience. Reference to the resolution section in this PSN for details and instructions.
 - <u>CVE-2021-45105 and CVE-2021-44832</u>: At the time of publishing this article, VMWare has not found a valid attack vector to exploit CVE-2021-45105 or CVE-2021-44832 in any VMware products. VMware has stated within the link below that "Going forward new log4j vulnerabilities will continue to be evaluated to determine severity and applicability to VMware products but will not be referenced in this advisory. VMware products will update open-source components (including log4j) to the latest available versions in future releases."

Reference to <u>VMSA-2021-0028.11</u> for further information.

• <u>CVE-2021-4104</u>: At the time of publishing this article the vendor has not released information regards to CVE-2021-4104 in their security advisory <u>VMSA-2021-0028.11</u>. VMware has stated within the link below that "Going forward new log4j vulnerabilities will continue to be evaluated to determine severity and applicability to VMware products but will not be referenced in this advisory. VMware products will update open-source components (including log4j) to the latest available versions in future releases."

✤ VMware ESXi 6.5.x

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

Extreme VSP 7024 Network Switches

- <u>CVE-2021-44228</u>: The BOSS OS running on the data switches is not impacted by CVE-2021-44228.
- <u>CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104:</u> 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 <u>VN-2021-465</u> for further information.

- Extreme VSP 4850 Network Switches
- <u>CVE-2021-44228</u>: The VOSS OS running on the data switches is not impacted by CVE-2021-44228.
- <u>CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104:</u> 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 <u>VN-2021-465</u> for further information.
- Extreme VSP 7254 Network Switches
 - <u>CVE-2021-44228</u>: The VOSS OS running on the data switches is not impacted by CVE-2021-44228.
 - <u>CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104:</u> 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
- <u>CVE-2021-44228 & CVE-2021-45046</u>: Impacted. New firmware has been released by the vendor; it uses Log4j 2.16 / JAVA 8.

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.

• <u>CVE-2021-45105</u>, <u>CVE-2021-44832</u>: At the time of publishing this article vendor is not aware of attackers exploting CVE-2021-45105 and CVE-2021-44832. Log4j **2.16** has also added a number of defense-in-depth protections against potential remote code execution issues that could impact customers. Given these two key factors, vendor is not working with a tighter timeline for distributing Log4j 2.17 or 2.17.1. Vendor's primary focus is set to mitigate CVE-2021-44228 and subsequently CVE-2021-45046.

Vendor will continue to monitor the impact of CVE-2021-45105, CVE-2021-4483 and any other issues discovered that may accelerate remedy timelines if circumstances change.

Reference to Dell Security Article <u>000194416</u> for further reference.

- <u>CVE-2021-4104</u>: At the time of publishing this article the vendor has not released information regards to CVE-2021-4104 to Security Articles <u>000194416</u> or <u>000194372</u> 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 <u>CVE-2021-44228 and subsequently CVE-2021-45046</u>.
- ✤ HPE/Nimble CS1000 Storage Array
- <u>CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104 & CVE-2021-44832:</u> Not Impacted. Reference to Customer Notice <u>a00120086</u> for further information.
- HPE DL360 Gen8 Servers / iLO4
- <u>CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104 & CVE-2021-44832:</u> Not Impacted. Reference to Customer Notice <u>a00120086</u> for further information.
- HPE DL360 Gen9 Servers / iLO4
- <u>CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104 & CVE-2021-44832:</u> Not Impacted. Reference to Customer Notice <u>a00120086</u> for further information.
- HPE DL360 Gen10 v1 and v2 Servers / iLO5
- <u>CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-4104 & CVE-2021-44832:</u> Not Impacted. Reference to Customer Notice <u>a00120086</u> for further information.

- Sentry 3 & 4 PDUs
- <u>CVE-2021-44228</u>: The firmware running on the PDUs is not impacted by CVE-2021-44228.
- <u>CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104:</u> 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 <u>https://www.servertech.com/support</u> for further information.
- ✤ Avaya Orchestrator 1.5
- <u>CVE-2021-44228</u>, <u>CVE-2021-45046</u>, <u>CVE-2021-45105</u>, <u>CVE-2021-44832</u> & <u>CVE-2021-4104</u>: 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 <u>https://www.nagios.com/news/2021/12/update-on-apache-log4j-vulnerability/</u> for further information.

- Management Server Console (MSC)
- <u>CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104</u>: Not impacted. The Windows Server 2016 OS that comes with the MSC OVA does not have any JAVA based application pre-installed.
- PDU Router
- <u>CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 & CVE-2021-4104:</u> 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: <u>DSA-2021-298</u>. See the Patch install instructions section below for the upgrade procedure. See the Download section for the PLDS ID for the new release file.
- <u>vCenter Server Appliance 6.5 Update U3s Build 19261680</u> permanently mitigates Log4j vulnerabilities CVE-2021-44228 and CVE-2021-45046. See the Patch install instructions section below for installation steps. See the download section for the PLDS ID for the new release file.

Workaround or alternative remediation

N/A

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.

Issue 6 – February 1, 2022: Update to the vCenter 6.5.x and VNXe3200 sections to include JAVA versions and other content shared from vendor website.

Issue7 – February 9, 2022: Note included for vCenter 6.5 updates for fix CVE-2021-44228 & CVE-2021-45046

Issue8 – February 22, 2022: Updates to vCenter Server Appliance 6.5 for CVE-2021-44228 & CVE-2021-45046

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# CPOD0000222 Patch install instructions

Dell/EMC VNXe3200 Storage Array upgrade to v3.1.17:

Software Release v3.1.17.10223906

Upgrade instructions:

<u>Important</u>: 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, etc), any issues must be fixed prior to attempting the upgrade activity.

<u>Warning</u>: 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.

<u>Note:</u> 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

Serviceinterrupting?

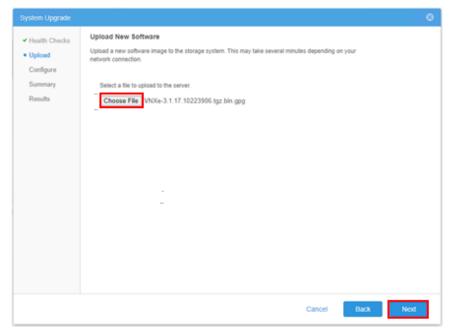
Yes

Settings				00
♀ Software and Licenses	System Informa	ation		
License Information Software Upgrades	Name:	cpd5-castl-fn10		
Disk Firmware	Model:	VNXe3200		
L Users and Groups	Serial Number: APM00154336094 Installed System Software			
🗐 Management	Software Type	Version	Release Date	
Storage Configuration	KityHawk+ OS	3.1.15.10216415	8/10/2021	
Q= Support Configuration	Upgrade Software	•		
≪ <mark>●</mark> Access	Perform Health	Checks Start Upgrade Do	vnload New Software	
Alerts				
			c	liose

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

Health Checks	Perform Health Checks	
Upload Configure Summary Results	It is recommended that you perform a system health check prior to starting the upgrade. This ensures the system is in a healthy and upgradable state. If there are issues that need attention, "Warning" and/or "Error" messages may be displayed.	
	Cancel New	đ

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.



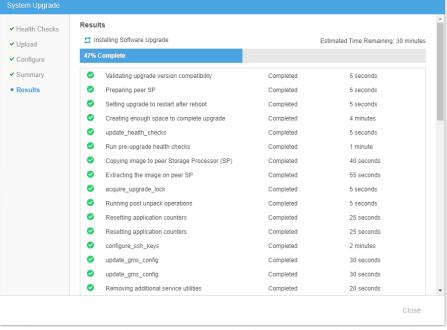
7. For the Configure Upgrade tab, leave as defaults, and click Next.

System Upgrade	
 ✓ Health Checks ✓ Upload ● Configure Summary Results 	Configure Upgrade ✓ Automatically Reboot Storage Processors Selecting this option will automatically reboot your storage processors during the upgrade and finalize the new software. Unselecting this option upgrade after all non-disruptive tasks have completed. User input is required to manually reboot the storage processors and finish the upgrade.
	Cancel Back 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.

System Upgrade		8
 Heath Checks. Upload Coofigure Summary Results 	Summary You are now ready to start the software upprade. This may take up to 90 minutes depending on configuration. All management operations will be disabled for the duration of the upgrade. Click the "Finish" button below to start the upgrade. Installed Software Version 3.1.0.10210415 Software Version 2.1.0.10210415 New Software Version The Aug 10 2021 23 22 22 GMT-0600 (Mountain Daylight Time) New Software Version 3.1.0.10219906 Software Type: Software Upgrade Rease Date: Start Dec 18 2021 19.42 24 GMT-0700 (Mountain Standard Time) Plantaming Start Dec 18 2021 19.42 24 GMT-0700 (Mountain Standard Time) Plantaming Yes Marcoline Yes Marcoline Yes Marcoline Yes	
	Cancel Back Finish	

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.

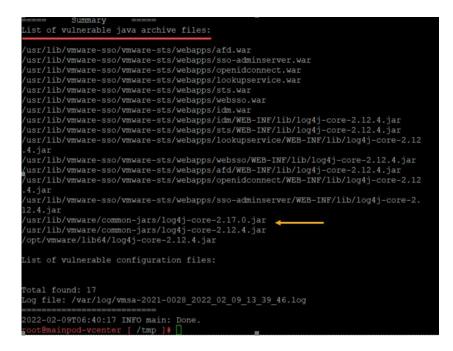
Health Checks	Results				
Upload	Software Upgrade Complete 100% Complete				
Configure	Nove Complete			-	
Summary	Validating upgrade version compatibility	Completed	5 seconds		
Results	Preparing peer SP	Completed	5 seconds		
	Setting upgrade to restart after reboot	Completed	5 seconds	- 1	
	 Creating enough space to complete upgrade 	Completed	4 minutes		
	update_health_checks	Completed	5 seconds		
	 Run pre-upgrade health checks 	Completed	1 minute		
	 Copying image to peer Storage Processor (SP) 	Completed	40 seconds		
	 Extracting the image on peer SP 	Completed	55 seconds		
	acquire_upgrade_lock	Completed	5 seconds		
	Running post unpack operations	Completed	5 seconds		
	acquire_upgrade_lock Running post unpack operations	Completed Completed	5 seconds	e	

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

Settings					00
Software and Licenses License Information • Software Upgrades Disk Firmware	System Informa Name: Modet: Serial Number: Installed System :	cpd5-cast VNXe320 APM0015	0		
Management Storage Configuration Support Configuration Access Access Alerts	Software Type KittyHawk+ OS Upgrade Software Perform Health (Version 3.1.17.10223906	Release Date 12/18/2021	
					Close

vCenter Server Appliance 6.5 Update 3s – Build 19261680:

 <u>Installation instructions:</u> Follow the same steps documented on to the latest MSC upgrade documentation for patching the vCenter server appliance to build 19261680-<u>Updating the vCenter Server Appliance section on page 76</u> <u>https://downloads.avaya.com/css/P8/documents/101070494</u> <u>Note:</u> DO NOT run the workaround mitigator script on vCSA build 19261680 as it has been developed to scan the configuration files for "-Dlog4j2.formatMsgNoLookups=true" and list the output without taking into account the Apache log4j versions running on the system. This will result in listing vulnerable java files even when these have been updated to 2.17.0 & 2.12.4 respectively.



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-2021-44832

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

Avaya Security Vulnerability Classification Reference <u>www.avaya.com/emergencyupdate</u> Mitigation As noted in this PSN.

If you require further information or assistance, please contact your Authorized Service Provider or visit <u>support.avaya.com</u>. 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 <u>Terms of Use</u>.

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.

All trademarks identified by [®] or TM are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners.