Product Support Notice

PSN #	PSN028000u				
Original publication date: 13-June-22. This is issue #01, published date: 13-June-22.	Severity/risk level	Medium	Urgency	When convenient	

Name of problem

PSN028000u – ASP 4200 4.x and 5.0 Spring Cloud Function & Spring4Shell vulnerabilities.

Products affected

Avaya Solutions Platform 4.x, ASP 4200 4.x, Avaya Solutions Platform 4200 5.0, ASP 4200 5.0

Problem description

Avaya is aware of the recently identified Spring Cloud Function and Spring4Shell (Spring Core Framework) vulnerabilities (CVE-2022-22963, CVE-2022-22965) and is conducting impact assessments across its portfolio, identifying opportunities for temporary mitigations, if possible, and developing plans for remediation, as appropriate. Reference the *Avaya Product Security* – ***Spring4Shell and Spring Cloud Function Vulnerabilities*** on support.avaya.com for updates.

ASP 4200 Releases and Impacts:

Avaya Solutions Platform 4200 4.x, Avaya Solutions Platform 5.0 – Impact assessment by CVE-2022-22963 and CVE-2022-22965

Individual component impact:

- VMware vCenter Server 6.5.x/7.0.x
  - **CVE-2022-22963 & CVE-2022-22965**: Not impacted.
    Reference to CVE-2022-22963 | Security | VMware Tanzu & VMSA-2022-0010 (vmware.com) for further information.

- VMware ESXi 6.5.x/7.0.x
  - **CVE-2022-22963 & CVE-2022-22965**: Not impacted.
    Reference to CVE-2022-22963 | Security | VMware Tanzu & VMSA-2022-0010 (vmware.com) for further information.

- Extreme VSP 7024 Network Switches
  - **CVE-2022-22963 & CVE-2022-22965**: The BOSS OS running on the switches is not impacted.
    Reference to Security Advisory: SA-2022-003 – "Spring4Shell" (CVE-2022-22965) | Extreme Portal (force.com) & Security Advisory: SA-2022-005 – Spring Cloud Function (CVE-2022-22963) | Extreme Portal (force.com) for further information.

- Extreme VSP 4850 Network Switches
  - **CVE-2022-22963 & CVE-2022-22965**: The VOSS OS running on the switches is not impacted.
    Reference to Security Advisory: SA-2022-003 – "Spring4Shell" (CVE-2022-22965) | Extreme Portal (force.com) & Security Advisory: SA-2022-005 – Spring Cloud Function (CVE-2022-22963) | Extreme Portal (force.com) for further information.

- Extreme VSP 7254 Network Switches
  - **CVE-2022-22963 & CVE-2022-22965**: The VOSS OS running on the switches is not impacted.
    Reference to Security Advisory: SA-2022-003 – "Spring4Shell" (CVE-2022-22965) | Extreme Portal (force.com) & Security Advisory: SA-2022-005 – Spring Cloud Function (CVE-2022-22963) | Extreme Portal (force.com) for further information.

- Dell/EMC VNXe3200 Storage Array

- **CVE-2022-22963 & CVE-2022-22965**: Not impacted.
  Reference to VNX, VNXe, Dell Unity: CVE-2022-22963 and CVE-2022-22965 Vulnerability (User Correctable) | Dell US for further information.

❖ Dell/EMC VNX5300 Storage Array
- **CVE-2022-22963 & CVE-2022-22965**: Not impacted.
  Reference to VNX, VNXe, Dell Unity: CVE-2022-22963 and CVE-2022-22965 Vulnerability (User Correctable) | Dell US for further information.

❖ HPE/Nimble CS1000 Storage Array
- **CVE-2022-22963 & CVE-2022-22965**: Not impacted.
  Reference to Document - Hewlett Packard Enterprise Critical Product Security Vulnerability Alerts | HPE Support for further information.

❖ HPE DL360 Gen8 Servers / iLO4
- **CVE-2022-22963 & CVE-2022-22965**: Not impacted.
  Reference to Document - Hewlett Packard Enterprise Critical Product Security Vulnerability Alerts | HPE Support for further information.

❖ HPE DL360 Gen9 Servers / iLO4
- **CVE-2022-22963 & CVE-2022-22965**: Not impacted.
  Reference to Document - Hewlett Packard Enterprise Critical Product Security Vulnerability Alerts | HPE Support for further information.

❖ HPE DL360 Gen10 v1 and v2 Servers / iLO5
- **CVE-2022-22963 & CVE-2022-22965**: Not impacted.
  Reference to Document - Hewlett Packard Enterprise Critical Product Security Vulnerability Alerts | HPE Support for further information.

❖ Sentry 3 & 4 PDUs
- **CVE-2022-22963 & CVE-2022-22965**: Not impacted.
  Server Technology 3rd-generation (Sentry3) CDU-series PDUs that run version 7.x firmware, and 4th-generation (Sentry4) PRO1- and PRO2-series that run version 8.x firmware, are not vulnerable to Spring4Shell (CVE-2022-22963, CVE-2022-22965). Server Technology's in-house custom-developed Network Interface Card (NIC) hardware and software application (OS) that runs these PDUs is built on top of a Digi International NET+OS Development Platform, and there is no Java component, no Spring Framework, so no vulnerability.

❖ Avaya Orchestrator 1.5
- **CVE-2022-22963 & CVE-2022-22965**: Not impacted. AO 1.5 builds do not use Spring / JAVA.

❖ Management Server Console (MSC) – Windows Server 2016 / 2019
- **CVE-2022-22963 & CVE-2022-22965**: Not impacted. Windows Server 2016/2019 does not use Spring / JAVA.

❖ PDU Router – Windows Server 2016 / RHEL 8.x
- **CVE-2022-22963 & CVE-2022-22965**: Not impacted.

Resolution

n/a

Workaround or alternative remediation

n/a

Remarks

n/a

Patch Notes

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

Backup before applying the patch

Always

Download

n/a

Patch install instructions

n/a

Service-interrupting?

No

Verification

n/a

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-2022-22965
Reference https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22963
Reference https://tanzu.vmware.com/security/cve-2022-22963
Reference https://tanzu.vmware.com/security/cve-2022-22965
Reference https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement
Reference https://blog.cloudflare.com/waf-mitigations-spring4shell/
Reference https://spring.io/blog/2022/04/01/spring-framework-rce-mitigation-alternative

Avaya Security Vulnerability Classification

Reference https://support.avaya.com/helpcenter/getGenericDetails?detailId=1399847128146

Mitigation

n/a

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.

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.