# Product Support Notice



PSN # PSN005939u



Original publication date: 15-Dec-21. This is issue #06, published date: 04-Feb-22.

Severity/risk level: High | Urgency: Immediately

**Name of problem**

Avaya Control Manager Log4j2 vulnerabilities (CVE-2021-44228/CVE-2021-45046/CVE-2021-45105/ CVE-2021-44832/CVE-2021-4104/CVE-2022-23302/CVE-2022-23305/CVE-2022-23307).

**Products affected**

Avaya Control Manager 9.0.2.x.

**Problem description**

Avaya is aware of the recently identified Apache Log4j2 vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, CVE-2021-44832 and CVE-2021-4104/CVE-2022-23302/CVE-2022-23305/CVE-2022-23307) 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.

| Avaya Control Manager Release | Impacted by CVE-2021-44228 | Impacted by CVE-2021-45046 | Impacted by CVE-2021-45105 | Impacted by CVE-2021-44832 | Impacted by CVE-2021-4104 | Impacted by CVE-2022-23302/CVE-2022-23305/CVE-2022-23307 |
|---|---|---|---|---|---|---|
| **9.0.2.1** | Yes. ACM Patch 9.0.2.1.1 upgrades Log4j to 2.16.0. | No. The SOLR component within ACM uses default configuration PatternLayout in the logging configuration and does not have Context lookups like ${ctx:loginId} or $${ctx:loginId}. Customers should not update this configuration. | No. The SOLR component within ACM uses default configuration PatternLayout in the logging configuration and does not have Context lookups like ${ctx:loginId} or $${ctx:loginId}. Customers should not update this configuration. | No. The SOLR component within ACM uses default configuration PatternLayout in the logging configuration and does not have Context lookups like ${ctx:loginId} or $${ctx:loginId}. Customers should not update this configuration. | No. Not using log4j 1.x | No. ACM 9.0.2.1 has log4j version 2.x which is not impacted. |
| **9.0.2.0.x** | Yes. ACM Patch 9.0.2.0.8 upgrades Log4j to 2.16.0. | No. The SOLR component within ACM uses default configuration PatternLayout in the logging configuration and does not have Context lookups like ${ctx:loginId} or $${ctx:loginId}. Customers should not update this configuration. | No. The SOLR component within ACM uses default configuration PatternLayout in the logging configuration and does not have Context lookups like ${ctx:loginId} or $${ctx:loginId}. Customers should not update this configuration. | No. The SOLR component within ACM uses default configuration PatternLayout in the logging configuration and does not have Context lookups like ${ctx:loginId} or $${ctx:loginId}. Customers should not update this | No. Not using log4j 1.x | No. ACM 9.0.2.1 has log4j version 2.x which is not impacted. |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | configuration. | | |
| **9.0.1.x** | No (9.0.1.x and older versions are using Log4j 1.x without JMSAppender configured and therefore not impacted by the vulnerability) | No (9.0.1.x and older versions are using Log4j 1.x without JMSAppender configured and therefore not impacted by the vulnerability) | No. (9.0.1.x and older versions are using Log4j 1.x without JMSAppender configured and therefore not impacted by the vulnerability) | No. (9.0.1.x and older versions are using Log4j 1.x without JMSAppender configured and therefore not impacted by the vulnerability) | No. ACM uses Log4j 1.6.1 without the JMSAppender configuration. The vulnerability affects Log4j 1.2.x when configured with non-default JMSAppender configuration. | No. Log4j is not configured to use JMSSink, JDBCAppender and ACM not shipping or using Chainsaw tool for viewing logs. |
| **9.0.0.x** | No (9.0.0.x and older versions are using Log4j 1.x without JMSAppender configured and therefore not impacted by the vulnerability) | No (9.0.0.x and older versions are using Log4j 1.x without JMSAppender configured and therefore not impacted by the vulnerability) | No. (9.0.1.x and older versions are using Log4j 1.x without JMSAppender configured and therefore not impacted by the vulnerability) | No. (9.0.1.x and older versions are using Log4j 1.x without JMSAppender configured and therefore not impacted by the vulnerability) | No. ACM uses Log4j 1.6.1 without the JMSAppender configuration. The vulnerability affects Log4j 1.2.x when configured with non-default JMSAppender configuration. | No. Log4j is not configured to use JMSSink, JDBCAppender and ACM not shipping or using Chainsaw tool for viewing logs. |

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

This PSN will be updated as more information is available. Please keep a link to this PSN handy for quick future reference and also sign up for e-Notifications on the Avaya Support site so that you are notified when this PSN is updated in the future.

## Resolution

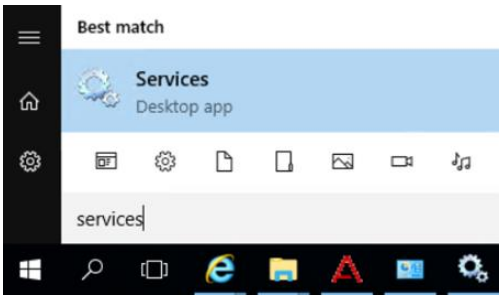
| Avaya Control Manager Release | Solution |
|---|---|
| 9.0.2.1 | ACM patch (9.0.2.1.1) has been released to address the vulnerabilities and can be downloaded from https://support.avaya.com. The patch will update ACM to utilize log4j2 version 2.16.0. Follow installation instructions in the patch readme contained in the patch zip. |
| 9.0.2.0.x | ACM patch (9.0.2.0.8) has been released to address the vulnerabilities and can be downloaded from https://support.avaya.com. The patch will update ACM to utilize log4j2 version 2.16.0. Follow installation instructions in the patch readme contained in the patch zip. |

## Workaround or alternative remediation

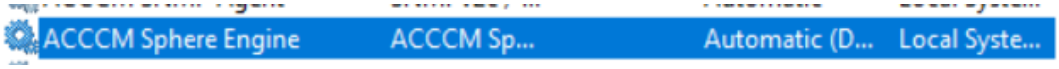
To mitigate the vulnerability, until the patch is installed, customers can stop the ACCCM Sphere service. The ACCCM Sphere service enables the search for specific entities, for example, a particular extension or VDN. Once the service is stopped this feature will not be available until the service is restarted.

Steps to stop the ACCCM Sphere service:

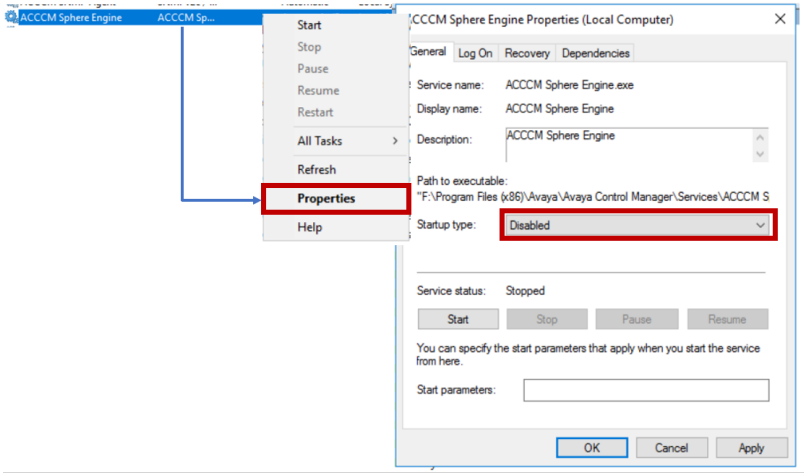
1. Logon to the ACM server with an admin account
2. Go to Start and search for ‘Services’:




3. On the Services application, stop the ACCCM Sphere Engine:




4. Right-click on the service, choose Properties and disable the service to avoid starting up inadvertently:




Once the patch has been installed, the ACCCM Sphere Engine service can once again be set to “Automatic (Delayed Start)” and service started.

| Remarks |
|---|
| Issue 1 – December 15, 2021: Initial publication. |
| Issue 2 – December 15, 2021: workaround and patch ETA updated. |
| Issue 3 – December 17, 2021: Patch released. |
| Issue 4 – December 20, 2021: Added details for CVE-2021-45105. |
| Issue 5 – January 7, 2022: Added details for CVE-2021-44832 and CVE-2021-4104. |
| Issue 6 – February 4, 2022: Added details for CVE-2022-23302/CVE-2022-23305/CVE-2022-23307 |

## 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** | **Service-interrupting?** |
| n/a | Yes |
| **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-2021-44228

CVSS Version 3.x Base Score: 10.0 Critical

CVSS Version 3.x Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

### 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.**