ActiveVideo®

15 December 2021

# CloudTV Product Bulletin:
# Log4j Vulnerability

ActiveVideo is aware of the recently identified log4j vulnerabilities, CVE-2021-44228 & CVE-2019-17571 & CVE-2021-45046 and has completed the evaluation of the impact to CloudTV platform components. Our investigation results showed no functional dependency on this library. The use of this library by CloudTV is for status and generic logging of internal components and not applicable to the network intrusion use cases identified in CVE-2021-44228 & CVE-2019-17571 & CVE-2021-45046. The CloudTV use of log4j version 1.2.8 is not applicable to CVE-2021-44228 which affects log4j versions 2.0 - 2.15. Hotfixes for CloudTV versions currently deployed at current customer sites, or versions eminent for deployment, will be compiled and made available for immediate release to customers. ActiveVideo will notify customers when the hotfix for your deployed version becomes available.

As an immediate step to avoid exposure to these identified vulnerabilities, we recommend upgrading the installed version of log4j to version 2.16 or to a release newer than 2.16 when available.

Reference:
https://nvd.nist.gov/vuln/detail/CVE-2021-45046
https://nvd.nist.gov/vuln/detail/CVE-2021-44228
https://nvd.nist.gov/vuln/detail/CVE-2019-17571
https://logging.apache.org/log4j/2.x/download.html

| Component | Platform version | log4j library dependency | log4j usage |
|---|---|---|---|
| CSM | * | - | - |
| SCM | * | - | - |
| LSM | * | - | - |
| Funnel | 2.9 / 2.16 / 2.22 | 1.2.16 | generic logging |
| UDC | 2.12<= | 1.2.16 | generic logging |
| UDC | 2.12<=  >=2.22 | 1.2.8 | no direct dependency |
| UDC | >=2.22 | 1.2.8 | formatting the layout of the ActiveMQ's logging to console |