



Apache Log4j exploits (CVE-2021-44228, CVE-2021-45046) and Omnicell Products

Updated 17 DEC 2021 1700 Pacific Time

Summary

A critical vulnerability in Apache Log4j (CVE-2021-44228) has been publicly disclosed that may allow for remote code execution. This component is widely used by both enterprise applications and Cloud services. Patch provided by Apache to address this also found to contain vulnerability (CVE-2021-45046)

Description

This vulnerability is also referred to as Log4j2, Log4Shell. Log4j library can also be included in a Java application as a transitive dependency with common Java libraries.

This issue only affects log4j versions between 2.0 and 2.14.1. The exploit requires an attacker to remotely access an endpoint and send arbitrary data logged or otherwise processed by the log4j engine.

Log4j vulnerability and Omnicell products

Following Omnicell products have been reviewed for Apache Log4j exploit (CVE-2021-44228 and CVE-2021-45046) and deemed either “Not impacted” or “Investigation complete”

OmniCenter Platform Solutions (All versions, All OS)	
OmniCenter	Not impacted
XT Automated Dispensing Cabinets	Not impacted
XT Controlled Substance Manager	Not impacted
XT Anesthesia Workstation	Not impacted
Previous generation of Automated Dispensing Cabinets	Not impacted
Patient Care Server	Not impacted
Central Pharmacy Manager	Not impacted
Central Pharmacy Workstation	Not impacted
XR2 Automated Central Pharmacy System	Not impacted



OmniCenter Platform – Continued	
Web applications on OmniCenter - AnywhereRN, OC Web, OC Analytics, SupplyX, MedX	Not impacted
Other server products	
OmniLinkRx Medication Order Management System	Not impacted
OmniceLL Pandora Analytics	Not impacted. See section “Known false positives by some security scanning systems”
OmniceLL Interface Services (OIS)	Not impacted
WorkFlow-Rx with Packager	Not impacted
Cloud Products	
OmniceLL One, OmniceLL Essentials, OmniceLL Telemetry Services	<p>UPDATE 12/17/2021: Cloud provider provided patch was applied to environment on 12/15/2021</p> <p>Previous update: Log4j is used on couple of Cloud components and updates are being scheduled. Meanwhile mitigations have been implemented by our Cloud/Services providers via modified Intrusion prevention rules to deny suspicious inbound traffic specific to this CVE, deny traffic from known exploit sources, additional log inspection rules to further detect and mitigate attempts to exploit</p>
Cloud Hosted OmniCenter	Not impacted
Hosted OmniCenter - Non-Acute Care	Not impacted
Guided Packing	Not impacted
SureMed X (Australia)	Not impacted
OmniceLL Proactive Monitoring and Remote Access	
vSuite for remote access (SecureLink)	Not impacted. Log4j core library (log4j-core) is not present in any classpaths. Other log4j dependencies do exist and this may result in false positives by some security scanning systems. See section “Known false positives by some security scanning systems”
IV Compounding Solutions	
IV Workflow Solutions (IVX Cloud, IVX Workflow)	Not impacted
IV Robotic Solutions (i.v.STATION, i.v.STATION ONCO)	Not impacted




Med Adherence Products	
OmniceLL Robotic Dispensing Systems (RDS)	Not impacted
OnDemand Servers, AccuFlex, E3	Not impacted
OnDemand Workstations	<p>UPDATE 12/17/2021 Investigation complete. Not impacted</p> <p>Previous update: Under investigation</p>
Connect-Rx Platform Solutions	
Connect-Rx Server	<p>UPDATE 12/17/2021 Investigation complete. A very small number of Connect-Rx servers at customer sites may contain ADC which is no longer used and can be uninstalled. See section below "Procedure to detect and remove ADC"</p> <p>Investigation of other components (COIL and Crystal Reports) is complete – Not impacted.</p> <p>Previous update</p> <p>Under investigation. Older non-vulnerable Log4j components may be present on Connect-Rx servers. If the files are dated year 2010, that version is not vulnerable. Log4j is used with proactive monitoring system ADC (Automated Data Collection), COIL and Crystal Reports on Connect-Rx server. Updates to follow along with uninstall or upgrade instructions</p>
DataStation, NarcStation, AcuDose systems	Not impacted. <i>Correction - earlier bulletin referred to Log4j on AcuDose systems. Log4j is not used on AcuDose</i>
Enterprise Medication Management (EMM)	Not impacted
OmniceLL Technology Solutions (SaaS)	
EnlivenHealth, FDS Ampicare, Omnicell 340B	Please contact your Account Manager



Known false positives by some security scanning systems

Some security scanning tools may incorrectly flag Omnicell systems or products as vulnerable to Log4j.

1. Log4j jar file in SecureLink folder

 log4j-over-slf4j-1.6.1.jar	Date modified: 7/24/2021 10:15 AM
C:\Program Files (x86)\SecureLink\bin\WEB-INF\lib	Type: JAR File
	Size: 12.0 KB

As explained above under “vSuite”, Log4j Core library (log4j-core) is not present in java class paths currently deployed by vSuite agent. Mere presence of file is not an indicator of vulnerability especially when it is not present in java class paths.

2. Log4j.jar file in customer provided SQL Server (Pandora servers)

Pandora product does not use Apache or Log4j but some customer provided SQL server used by Pandora application may have Log4j in SQL Server extensions folder.

Plugin Output

```
Path           : C:\Program Files (x86)\Microsoft SQL Server\150\DTS\Extensions
\Common\Jars\log4j-1.2.17.jar
  Installed version : 1.2.17
  Fixed version    : 2.15.0
```

Customer IT/DBA should evaluate need for DTS and upgrade or remove if necessary. Unlike other turnkey Omnicell solutions, Pandora servers are provisioned and managed by customer IT departments.



Connect-Rx Servers: Procedure to detect and remove ADC

ADC (Automated Data Collection) is no longer used on Connect-Rx server but a very small number of Connect-Rx customer servers may still have the agent running which uses Log4j. Please follow below instructions to detect if ADC exists and if so uninstall ADC.

Step 1: Check if ADC exists on Connect-Rx Server

Search for ADCEngine.exe – default location is c:\crx\service\ADCEngine. While unlikely this file may exist in other location on the drive so please search whole system.

Step 2: If ADCEngine.exe is found, follow below steps to uninstall

- a. Open a command prompt as administrator (“Run as Administrator”)
- b. Type `c:`
- c. Type `cd \crx\service\adcengine\bin`
- d. Type `adcengine -remove`

Note:

- If you get a message saying - “OpenSCManager failed - Access is denied.” - This means that your command prompt was not run as Administrator.
- If you get a message saying - “OpenService failed - The specified service does not exist as an installed service.” - This means ADC service has already been removed

- e. Type `cd \crx\service`
- f. Type `rd /s ADCEngine`

if ADCEngine.exe is found in another location/drive, please do the same procedure as above modifying the locations in (b) thru (d)

If you have additional questions please contact Omnicell Technical Assistance Center. Further updates to this bulletin will also be available on myOmnnicell.com

- Submit ticket on customer portal myOmnnicell.com
- Submit ticket via OC-Care Mobile App
- Call 24x7 Support at appropriate phone number listed at <https://www.omnicell.com/product-support>

GK-12172021-v3