Apache Log4j exploit (CVE-2021-44228) and Omnicell Products

Updated 12/14/2021 2100 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.

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 deemed either “Not impacted” or “Under investigation”

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
Web applications on OmniCenter - AnywhereRN, OC Web, OC Analytics, SupplyX, MedX	Not impacted

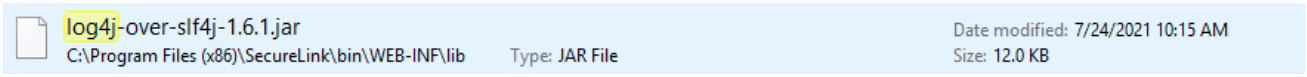
Other server products	
OmniLinkRx Medication Order Management System	Not impacted
Omnicell Pandora Analytics	Not impacted. *See section "Known false positives by some security scanning systems"*
Omnicell Interface Services (OIS)	Not impacted
WorkFlow-Rx with Packager	Not impacted
Cloud Products	
Omnicell One, Omnicell Essentials, Omnicell Telemetry Services	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
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	Under investigation

Connect-Rx Platform Solutions	
Connect-Rx Server	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
DataStation, NarcStation, AcuDose systems	Not impacted. *Correction - earlier bulletin referred to Log4j on AcuDose systems. Log4j is not used on AcuDose*
Enterprise Medication Management (EMM)	Not impacted
Omnicell Technology Solutions	
EnlivenHealth, FDS Amplicare, 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



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.

Omnicell

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.

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

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

GK-12142021-v2