AUTHOR(S)	:	OpenScape Baseline Security Office
DOCUMENT NUMBER	:	N.A
VERSION	:	1.2
STATUS	:	Final
SOURCE	:	Atos
DOCUMENT DATE	:	
NUMBER OF PAGES	:	11

Contents

List of changes

version	Date	Description	Author(s)
1.0	14 December 2021	Document created	OSCC Development
1.1	15 December 2021	Added Email Relay Component, add CVE-2021-4104 statement and small updates	OSCC Development
1.2	21 December 2021	Small updates requested by GVS to avoid misunderstandings	OSCC Development

1 OpenScape Contact Center Solution Log4j Critical vulnerability Log4Shell (CVE-2021-44228)

The OpenScape Contact Center solution has some components with a vulnerable version of log4j2.
In the next releases the vulnerability will be fixed with at least log4j2 version 2.16.0.
While those releases are not available, customers who desire to be protected can follow the steps in this article, see chapters 3 through 5, as workaround.
The workarounds are presented per affected services and systems.

The OSCC versions affected are V9, V10 and V11.

2 OpenScape Contact Center Solution Log4j Critical vulnerability (CVE-2021-4104)

The OpenScape Contact Center solution is not affected by this vulnerability, as the JMSAppender is not used.

3 OpenMedia Connectors

Some components use a vulnerable version of Log4j2.
Below there are procedures to protect the services.

3.1 Elasticsearch

The OpenMedia connectors depend on the Elasticsearch service. This service uses a vulnerable version of Log4j2.

To work around the vulnerability, execute the following steps:

Stop Elasticsearch service

Go to Elasticsearch bin folder and execute the command:

elasticsearch-service.bat manager

If the Elasticsearch is installed in default path execute the command:

"C:\Program Files\OpenScape\Contact Center\Elasticsearch\bin\elasticsearch-service.bat" manager

It will open a GUI to edit the Elasticsearch service.

Go to tab "Java" and in the Java Options add the line:

-Dlog4j2.formatMsgNoLookups=true

Start Elasticsearch service

Reference:
https://discuss.elastic.co/t/is-elasticsearch-affected-by-cve-2021-45046-a-second-vulnerability-in-log4j/291885

3.2 Whatsapp Connector

The instructions to apply this workaround in the whatsapp-connector are the following:

Stop OsccWhatsAppConnector service

Edit the file WhatsAppConnector.xml. The default path for this file is "C:\Program Files\OpenScape\Contact Center\OpenMedia\whatsapp-connector". In the tag arguments add the parameter:

-Dlog4j2.formatMsgNoLookups=True

The result after the change should be:

<arguments>-Dcom.ibm.jsse2.overrideDefaultTLS=true
-Dcom.ibm.jsse2.overrideDefaultProtocol=TLSv12 -jar whatsapp-connector-server-1.0.jar
-spring.config.name=waconnector **-Dlog4j2.formatMsgNoLookups=True**</arguments>

Start OsccWhatsAppConnector service

3.3 Twitter Connector:

The instructions to apply this workaround in the twitter-connector are the following:

Stop OsccTwitterConnector service

Edit the file TwitterConnector.xml. The default path for this file is "C:\Program Files\OpenScape\Contact Center\OpenMedia\twitter-connector". In the tag arguments add the parameter:

-Dlog4j2.formatMsgNoLookups=True

The result after the change should be:

<arguments>-Dcom.ibm.jsse2.overrideDefaultTLS=true
-Dcom.ibm.jsse2.overrideDefaultProtocol=TLSv12 -jar twitter-connector-server-1.0.jar
-Dlog4j2.formatMsgNoLookups=True</arguments>

Start OsccTwitterConnector service

4 OpenScape Contact Center Server (OSCC)

4.1 Openfire Service

On OSCC server the Openfire Service uses a vulnerable Log4J2 version. To protect the system, execute the workaround below.

The instructions to apply this workaround in the openfire are the following:

Stop Openfire service

Edit the file %HPPCDIR%OpenFire\bin\openfire-service.vmoptions and add the line:

-Dlog4j2.formatMsgNoLookups=true

Note: If the file doesn't exist, create it and ensure the name of file doesn't have additional extension like ".txt". The file extension must be ".vmoptions".

Start Openfire service

Reference:

https://discourse.igniterealtime.org/t/openfire-4-6-5-released/91108

4.2 OpenScape Contact Center Application Server with Web Interaction SDK

The only affected component on OSCC Application Server is Web Interaction SDK, because it uses a vulnerable Log4J2 version.

The Web Interaction SDK can be installed either on a dedicated Apache Tomcat server or on the Apache Tomcat server of the OSCC Application Server.

Note: Other applications of the OSCC Application Server, like Agent Portal Web, are not affected. So, if the Web Interaction SDK is not used, then the workaround below is not applicable.

Note: We are providing the workaround for the OSCC Application Server.

If the Web Interaction SDK is used, then the instructions to apply the workaround on the Apache Tomcat server of the OSCC Application Server are the following:

Stop OpenScape Contact Center Application Server service

For execute the file:

"%OSCCAppServerLocation%\ApplicationServer\ApacheWebServer\bin\tomcat9w.exe"

Or

"%OSCCAppServerLocation%\ApplicationServer\ApacheWebServer\bin\tomcat8w.exe"

It will open a GUI to edit the Tomcat service.

Go to tab "Java" and in the Java Options add the line:

-Dlog4j2.formatMsgNoLookups=true

Start OpenScape Contact Center Application Server service

4.3 OpenScape Contact Center Email Relay

On OSCC server the Email Relay Service uses a vulnerable Log4J2 version. To protect the system, execute the workaround below.

Stop OsccEmailRelay service

Edit the file EmailRelayService.xml. The default path for this file is "C:\Program Files\OpenScape\Contact Center\EmailRelay". In the tag arguments add the parameter:

-Dlog4j2.formatMsgNoLookups=True

The result after the change should be:

<arguments>**-Dlog4j2.formatMsgNoLookups=true** -jar email-relay.jar</arguments>

Start OsccEmailRelay service

5 OpenScape Contact Media Service (OSCMS)

5.1 OSCMS all versions

The OSCMS server uses a vulnerable version of Log4j2.

The workarounds below help to mitigate the vulnerability manually.

Logon to CMS system with root privileges.

Stop the CMS service with the commands:

service cmsserver stop

Using vi editor edit the file:

/opt/cmsserver

Add the java -Dlog4j2.formatMsgNoLookups=true argument to the javaArgs property.

The property should be like this:
javaArgs="**-Dlog4j2.formatMsgNoLookups=true** -Xmx2048m -Dfile.encoding=en_US.UTF-8 -jar /opt/Core/application_host/bin/apphost-starter.jar daemon"

Start the CMS service with the commands:

service cmsserver start

5.2 OSCMS Version 11 with Outbound Dialer enabled

The OSCMS Outbound Dialer uses a vulnerable version of Log4j2.

The workarounds below help to mitigate the vulnerability manually.

Logon to CMS system with root privileges.

Stop the Outbound Dialer services with the commands:
service dialer stop
service dialerdnc stop

Using vi editor edit the files:

/opt/cms/dialer/dialer.service

/opt/cms/dialer/dnc/dialerdnc.service

Add the java -Dlog4j2.formatMsgNoLookups=true argument to the **ExecStart** property.

The property should be like this:
ExecStart=/opt/ibm/java/jre/bin/java -Xmx1024m -Dfile.encoding=en_US.UTF-8 **-Dlog4j2.formatMsgNoLookup=true**

Start the dialer services with the commands:

service dialer start
service dialerdnc start