

Atlas Copco	Atlas Copco BLM s.r.l.	Service Procedure	
	Approval date: 20-12-2021	version: 1	Page: 1 of 5
Title: QA Supervisor SERVICE PROCEDURE 22 – Temporary solution for VULNERABILITY CVE-2021-44228			


1 AIM

This document describes how to temporary fix the vulnerability CVE-2021-4428.

CVE-2021-44228 (also identified as Log4Shell) is a critically rated vulnerability affecting Log4j 2 (Java log manager) which is integrated into Apache’s web server suite. It impacts Apache Log4j 2 versions 2.0 through 2.14.1.

Index

1	AIM.....	1
2	REQUIREMENTS	2
3	PROCEDURE	2
	3.1 STOPPING THE SERVICE.....	2
	3.2 ADDING A NEW PROPRIETY.....	2
	3.3 UPDATING LOG4J MODULES	2
	3.4 DISABLING LOG CONFIGURATION	3
	a. STANDALONE	3
	b. LOG4J2.xml files	4
	3.5 RESTARTING THE SERVICE	5

	Atlas Copco BLM s.r.l.	Service Procedure		
	Approval date: 20-12-2021	version: 1	Page: 2 of 5	
Title: QA Supervisor SERVICE PROCEDURE 22 – Temporary solution for VULNERABILITY CVE-2021-44228				

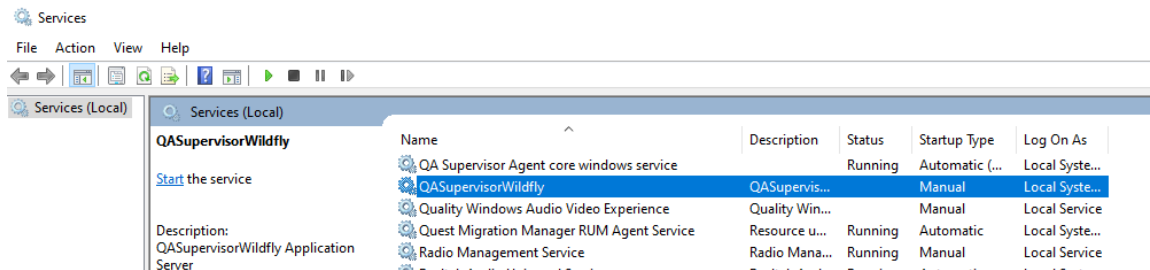
2 REQUIREMENTS

- All QA Supervisor versions prior to **06.03b** are affected
- Access to the server where QA Supervisor is installed
- Privilege to modify the files in the QA Supervisor installation path

3 PROCEDURE

3.1 STOPPING THE SERVICE

1. Access the server where QA Supervisor is installed and open the Windows services popup.



2. Stop QASupervisorWildfly service.

3.2 ADDING A NEW PROPRIETY

3. Open the folder *C:\Program Files\Atlas Copco Tools AB\QASupervisor\application\wildfly\bin*
4. Open the **standalone.conf.bat** file with a text editor and administration rights.

5. Find the line:

```
set "JAVA_OPTS=%JAVA_OPTS% -Dlog4j.configurationFile=\\\"%JBASS_HOME%...\configuration\log4j2.xml\\""
```

6. Add a new line after the one found, and paste the following text:

```
set "JAVA_OPTS=%JAVA_OPTS% -Dlog4j2.formatMsgNoLookups=true"
```



NOTE: This is how the file should be.

```
set "JAVA_OPTS=%JAVA_OPTS% -Djavax.ws.rs.ext.RuntimeDelegate=org.jboss.resteasy.spi.ResteasyProviderFacto
set "JAVA_OPTS=%JAVA_OPTS% -Dlog4j.configurationFile=\\\"%JBASS_HOME%...\configuration\log4j2.xml\\"
set "JAVA_OPTS=%JAVA_OPTS% -Dlog4j2.formatMsgNoLookups=true"
set "JAVA_OPTS=%JAVA_OPTS% -Dorg.jboss.logging.provider=log4j2"
set "JAVA_OPTS=%JAVA_OPTS% -Djava.library.path=\\\"%JBASS_HOME%...\libs\\";\\\"%JBASS_HOME%...\license\\"";
set "JAVA_OPTS=%JAVA_OPTS% -DANTLR_USE_DIRECT_CLASS_LOADING=true";
```

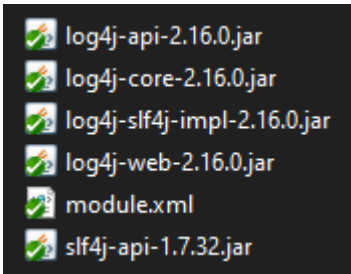
7. Save and close the file.

3.3 UPDATING LOG4J MODULES

8. Open the folder *C:\Program Files\Atlas Copco Tools AB\QASupervisor\application\wildfly\modules\org\apache\logging\log4j\main*
9. Delete the content of that folder.
10. Extract and copy the content from zip file [*main.zip*] in the same path.

Atlas Copco	Atlas Copco BLM s.r.l.	Service Procedure	
	Approval date: 20-12-2021	version: 1	Page: 3 of 5
Title: QA Supervisor SERVICE PROCEDURE 22 – Temporary solution for VULNERABILITY CVE-2021-44228			

11. Here is how the content should look like:



3.4 DISABLING LOG CONFIGURATION

a. STANDALONE

12. Open the folder *C:\Program Files\Atlas Copco Tools AB\QASupervisor\application\wildfly\standalone\configuration*
13. Open with an editor the file *standalone.xml*
14. Find the line with *urn:jboss:domain:logging*

```

<profile>
  <subsystem xmlns="urn:jboss:domain:logging:6.0">
    <console-handler name="CONSOLE">
      <level name="INFO"/>
      <formatter>
        <named-formatter name="COLOR-PATTERN"/>
      </formatter>
    </console-handler>
  </subsystem>
</profile>

```

15. In the following SUBSYSTEM section, replace all the level name="XXX" with level name="OFF"

Atlas Copco	Atlas Copco BLM s.r.l.	Service Procedure	
	Approval date: 20-12-2021	version: 1	Page: 4 of 5
Title: QA Supervisor SERVICE PROCEDURE 22 – Temporary solution for VULNERABILITY CVE-2021-44228			

16. The result should look like the following:

```

<subsystem xmlns="urn:jboss:domain:logging:6.0">
  <console-handler name="CONSOLE">
    <level name="OFF"/>
    <formatter>
      <named-formatter name="COLOR-PATTERN"/>
    </formatter>
  </console-handler>
  <size-rotating-file-handler name="FILE" autoflush="true">
    <formatter>
      <named-formatter name="PATTERN"/>
    </formatter>
    <file relative-to="jboss.server.log.dir" path="../../>
    <rotate-size value="15m"/>
    <max-backup-index value="9"/>
    <append value="false"/>
  </size-rotating-file-handler>
  <logger category="org.jboss.as.ejb3.timer">
    <level name="OFF"/>
  </logger>
  <logger category="org.hibernate.orm.deprecation">
    <level name="OFF"/>
  </logger>
  <logger category="org.apache.tika">
    <level name="OFF"/>
  </logger>
  <logger category="com.arjuna">
    <level name="OFF"/>
  </logger>
  <logger category="org.jboss.as.config">
    <level name="OFF"/>
  </logger>
  <logger category="sun.rmi">
    <level name="OFF"/>
  </logger>
  <root-logger>
    <level name="OFF"/>
    <handlers>
      <handler name="FILE"/>
    </handlers>
  </root-logger>

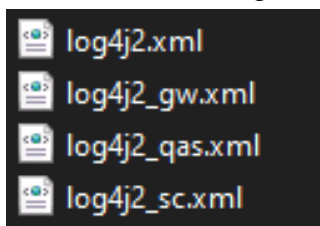
```

17. Save and close the file.

b. LOG4J2.xml files


18. Open the folder *C:\Program Files\Atlas Copco Tools AB\QASupervisor\configuration*

19. Delete the following files



20. Extract and copy the content from zip file [logs.zip] in the same path

21. The deleted files should have been restored from the zip file.

	Atlas Copco BLM s.r.l.	Service Procedure	
	Approval date: 20-12-2021	version: 1	Page: 5 of 5
Title: QA Supervisor SERVICE PROCEDURE 22 – Temporary solution for VULNERABILITY CVE-2021-44228			

3.5 RESTARTING THE SERVICE

22. Restart the QASupervisorWildfly service.