YSOFT SAFEQ LOG4J VULNERABILITY - PRODUCT UPDATE/WORKAROUND

We are aware of the current vulnerability in one widely used Java logging library: Apache Log4j. This library is a de-facto market standard for logging and troubleshooting Java applications with millions of applications using this library worldwide. YSoft SAFEQ is one of them. This vulnerability has been reported and tracked as CVE-2021-44228 (mitre.org) and CVE-2021-44228 (nist.gov).

Note that Y Soft is working to release SAFEQ build 64 which will entirely mitigate the Apache Log4j vulnerability. The release date for build 64 will be communicated on December 14. Prior to the availability of YSoft SAFEQ build 64, the following details the proper mitigation process. Note that SAFEQ Cloud is not impacted. YSoft SAFEQ Managed customers will be proactively contacted by Y Soft customer support to mitigate the SAFEQ Managed environment.

As communicated earlier today, we are following up with mitigation options.

SAFEQ Version	**Vulnerable**	**Mitigation**
SAFEQ 4	No	Not required
SAFEQ 5	No	Not required
SAFEQ 6 up to B44	Yes	Sections 1.1, 1.2
SAFEQ 6 B45 up to B63	Yes	Sections 1.3, 1.4
SAFEQ 6 B64 (release pending)	No	Release date will be announced tomorrow.
Data Protection Tool included in SAFEQ 6 (all versions)	YES	Section 1.3

1. HOW TO MITIGATE THE VULNERABILITY

This section describes the steps required to mitigate this vulnerability until a permanent fix is released in SAFEQ 6 B64.

1.1. TURN OFF LOGGING FOR ALL SAFEQ COMPONENTS

If your SAFEQ 6 is build 44 or older, as a security precaution, we recommend temporarily disabling all logging that is done via the vulnerable log4j library. This is a strictly temporary measure and as soon as we release the library patch script (to be released on December 14, 2021), this will no longer be necessary.
This requires the reconfiguration of several SAFEQ components, which is done in the following configuration files (assuming C:\SafeQ6 is your installation root):

- C:\SafeQ6\Management\conf\log4j2.xml
- C:\SafeQ6\Management\conf\log4j2-cmldbs.xml
- C:\SafeQ6\Management\conf\replicator\log4j2.xml
- C:\SafeQ6\Management\utilities\data-protection-cli\conf\log4j2.xml
- C:\SafeQ6\Management\validator\conf\log4j2.xml
- C:\SafeQ6\SPOC\conf\log4j2.xml
- C:\SafeQ6\SPOC\conf\log4j2-ors_fresh_start.xml
- C:\SafeQ6\SPOC\distServer\config\log4j2.xml

To disable logging via log4j, we essentially need to disable the Root logger in each of the configuration files. This is done by setting the Root logger level to “off”, as in:

```
<Root level="off">
   <AppenderRef ref="management_log_app"/>
</Root>
```

for each SAFEQ component/service. The configuration files are plain text files, and you can use your favorite text editor or the Notepad app included in Windows and Windows Server installs. The individual configuration files are shown in the following table.
Each service requires a restart once the corresponding configuration files are updated in the log4j configuration files for each component. Logging can be completely turned off by setting the root logger level to off.

Windows Service Name	Configuration File	How the File Should Look After the Edit	Notes
YSoft SAFEQ Management Service	C:\SafeQ6\Management\conf\log4j2.xml	<Root level="off"> <AppenderRef ref="management_log_app"/> </Root>	
YSoft SAFEQ Management Service	C:\SafeQ6\Management\conf\log4j2-cmldbs.xml	<Root level="off"> <AppenderRef ref="log_app"/> </Root>	
YSoft SAFEQ Management Service	C:\SafeQ6\Management\validator\conf\log4j2.xml	<Root level="off"> <AppenderRef ref="file_app"/> </Root>	Database Validation is not a standalone service.
YSoft SAFEQ LDAP Replicator	C:\SafeQ6\Management\conf\replicator\log4j2.xml	<Root level="off"> <AppenderRef ref="ldap_replicator_log_app"/> </Root>	
Data Protection Utility	C:\SafeQ6\Management\utilities\data-protection-cli\conf\log4j2.xml	<Root level="off"> <AppenderRef ref="file_app"/> </Root>	Data Protection Utility is not a service and does not require a restart.
YSoft SAFEQ Spooler Controller	C:\SafeQ6\SPOC\conf\log4j2.xml	<Root level="off"> <AppenderRef ref="log_app"/> </Root>	
YSoft SAFEQ Spooler Controller	C:\SafeQ6\SPOC\conf\log4j2-ors_fresh_start.xml	<Root level="off"> <AppenderRef ref="console_app"/> </Root>	
YSoft SafeQ Spooler Controller Group Service	C:\SafeQ6\SPOC\distServer\config\log4j2.xml	<Root level="off"> <!--AppenderRef ref="console_app"/--> <AppenderRef	This service does not require a manual restart as it is started from Y Soft SAFEQ

		ref="log_app"/> </Root>	Spooler Controller. Please restart those services instead.
YSoft SAFEQ Job Service Distributed Layer	C:\SafeQ6\JobService\distServer\config\log4j2.xml	<Root level="off"> <!--AppenderRef ref="console_app"/--> <AppenderRef ref="log_app"/> </Root>	

1.2. TURN OFF LOGGING AUTOMATICALLY USING POWERSHELL

If you do not want to edit files manually and you are able to use PowerShell, such as the version bundled with Microsoft Windows Server, you can use the following short script. Do not forget to replace “C:\SafeQ6” with your installation root folder.

```
$configFiles = (Get-ChildItem -Path "C:\SafeQ6" -Include "log4j*.xml" -Recurse).FullName
foreach ($file in $configFiles)
{
   $date = (Get-Date -UFormat %s)
   $backupFile = "${file}.${date}.bak"
   Write-Host "Patching file: ${file}, creating backup ${backupFile}"
   Copy-Item -Path $file -Destination $backupFile
   (Get-Content $file) | Foreach-Object { $_ -replace '<Root level="(info|debug|fatal|error|all|warn|trace)">', '<Root level="off">' } | Set-Content $file
}
```

1.3. TURN OFF LOGGING FOR THE DATA PROTECTION TOOL ONLY

If your installation does not require the disabling of all logging and you only need to disable logs for the Data Protection Tool, you need to update the following configuration file.

Data Protection Utility	**C:\SafeQ6\Management\utilities\data-**	**<Root level="off"> <AppenderRef**	**Data Protection Utility is not a service and**

	protection-cli\conf\log4j2.xml	**ref="file_app"/> </Root>**	**does not require a restart.**

1.4. DISABLE THE VULNERABLE LOOKUPS IN LOG4J

Starting with SAFEQ 6 B45, the vulnerability can be mitigated with the reconfiguration of the log4j logging library. Instead of disabling the logs, service configurations are updated to disable the vulnerable functionality in the log4j library.

Windows Service Name	**How to Change the log4j Configuration**
Management	1. Open Windows Command Line (cmd.exe, Terminal, PowerShell). 2. Navigate to SafeQ 6 Management Service installation root (e.g., C:\SafeQ6\Management). 3. Go to tomcat\bin sub directory (C:\SafeQ6\Management\tomcat\bin). 4. Run the following command from the command line: tomcat9.exe //US//YSoftSQ-Management ++JvmOptions=-Dlog4j2.formatMsgNoLookups=true 5. Restart the YSoftSQ-Management (YSoft SafeQ Management Service) service. **You can accomplish the entire producedure with the following commands:** C:\SafeQ6\Management\tomcat\bin\tomcat9.exe //US//YSoftSQ-Management ++JvmOptions=-Dlog4j2.formatMsgNoLookups=true C:\SafeQ6\Management\tomcat\bin\tomcat9.exe //SS//YSoftSQ-Management C:\SafeQ6\Management\tomcat\bin\tomcat9.exe //RS//YSoftSQ-Management
YSoft SAFEQ Spooler Controller	6. Navigate to SPOC installation root (e.g., C:\SafeQ6\SPOC)

<table>
<tr><td></td><td>7. Go to the bin subdirectory and edit the wrapper.conf file (e.g., C:\SafeQ6\SPOC\bin\wrapper.conf).
8. Add the following line wrapper.java.additional.21 = -Dlog4j2.formatMsgNoLookups=true
The configuration file contains several lines starting with the wrapper.java.additional prefix, each with a unique, increasing number after the dot. Please replace the number 21 above with the next number following the last number used in your configuration.
If your last entry is wrapper.java.additional.7, your new entry will say wrapper.java.additional.8.
9. Restart the YSoftSQ-SPOC (YSoft SAFEQ Spooler Controller) service.</td></tr>
<tr><td>YSoft SAFEQ Spooler Controller Group Service</td><td>10. Open Windows Command Line (cmd.exe, Terminal, PowerShell).
11. Navigate to the SPOC installation root (C:\SafeQ6\SPOC).
12. Go to the distServer\bin subdirectory (e.g., C:\SafeQ6\SPOC\distServer\bin).
13. Run prunsrv.exe //US//YSoftSQ-SPOCGS ++JvmOptions=-Dlog4j2.formatMsgNoLookups=true
14. Restart the YSoftSQ-SPOCGS (YSoft SAFEQ Spooler Controller Group Service).
You can accomplish the entire procedure with the following commands:
C:\SafeQ6\SPOC\distServer\bin\prunsrv.exe //US//YSoftSQ-SPOCGS ++JvmOptions=-Dlog4j2.formatMsgNoLookups=true
C:\SafeQ6\SPOC\distServer\bin\prunsrv.exe //SS//YSoftSQ-SPOCGS
C:\SafeQ6\SPOC\distServer\bin\prunsrv.exe //RS//YSoftSQ-SPOCGS</td></tr>
<tr><td>YSoft SAFEQ LDAP Replicator</td><td>15. Open Windows Command Line (cmd.exe, Terminal, PowerShell).</td></tr>
</table>

<table>
<tr>
<td></td>
<td>
16. Navigate to the SAFEQ 6 Management installation root (C:\SafeQ6\Management).
17. Go to the ldapreplicator subdirectory (C:\SafeQ6\Management\ldapreplicator).
18. Run ldap-replicator-wrapper.exe //US//YSoftSQ-LDAP ++JvmOptions=-Dlog4j2.formatMsgNoLookups=true
19. Restart the YsoftSQ-LDAP (YSoft SafeQ LDAP Replicator) service.
You can accomplish the entire procedure with the following commands:
<pre>C:\SafeQ6\Management\ldapreplicator\ldap-replicator-wrapper.exe //US//YsoftSQ-LDAP ++JvmOptions=-Dlog4j2.formatMsgNoLookups=true
C:\SafeQ6\Management\ldapreplicator\ldap-replicator-wrapper.exe //SS//YsoftSQ-LDAP
C:\SafeQ6\Management\ldapreplicator\ldap-replicator-wrapper.exe //RS//YsoftSQ-LDAP</pre>
</td>
</tr>
<tr>
<td>YSoft SafeQ Job Service Distributed Layer</td>
<td>
20. Open Windows Command Line (cmd.exe, Terminal, PowerShell).
21. Navigate to the SAFEQ 6 Job Service installation root (C:\SafeQ6\JobService).
22. Go to the procrun subdirectory (C:\SafeQ6\JobService\procrun).
23. Run prunsrv.exe //US//YSoftSQ-JSDL ++JvmOptions=-Dlog4j2.formatMsgNoLookups=true
24. Restart the YSoftSQ-JSDL (YSoft SAFEQ Job Service Distributed Layer) service.
You can accomplish the entire procedure with the following commands:
<pre>C:\SafeQ6\JobService\procrun\prunsrv.exe //US//YSoftSQ-JSDL ++JvmOptions=-Dlog4j2.formatMsgNoLookups=true
C:\SafeQ6\JobService\procrun\prunsrv.exe //SS//YSoftSQ-JSDL</pre>
</td>
</tr>
</table>

	C:\SafeQ6\JobService\procrun\prunsrv.exe //RS//YSoftSQ-JSDL