YSOFT SAFEQ®

LOG4J ANNOUNCEMENT

CONTENT

Applies to
YSoft SAFEQ 6
YSoft SAFEQ 5

1 SUMMARY

Y Soft is closely monitoring the evolving situation around the Apache Log4j vulnerabilities and providing up-to-date security advisory whenever the situation develops. Log4j library is a de facto market standard for logging and troubleshooting Java applications with countless applications using this library worldwide. YSoft SAFEQ is one of them. Apache has acknowledged these vulnerabilities and has released patched versions that are mitigating them.

The most discussed vulnerabilities are:

CVE-2017-5645 CVE-2019-17571
CVE-2020-9488 CVE-2021-4104
CVE-2021-44228 (CRITICAL, see explanation below) CVE-2021-44832 CVE-2021-45046 (CRITICAL, see explanation below) CVE-2021-45105

We consider a vulnerability CRITICAL when it has a high base score on nist.gov and, at the same time, it can be exploited remotely without full access to the filesystem of the server. We do NOT consider a vulnerability as CRITICAL if the the vulnerable class is present in Y Soft products, but it is not used by default or with any settings advised by our documentation – the attacker would need full access to the filesystem of the server (.xml/.conf files) and to Windows services to enable the problematic part of the code. Moreover, if the attacker was able to obtain full access to the server, the ability to misuse the vulnerability would be the least of everyone's concerns.

2 RESOLUTION

This is the list of YSoft SAFEQ versions and their mitigation steps:

SAFEQ Version	Vulnerable to any CVE listed above	Vulnerable to any CRITICAL CVE listed above	Recommendation
SAFEQ 4	Yes	No	N/A
SAFEQ 5 MU 48 or older	Yes	No	Update to SAFEQ 5 MU101 or newer
SAFEQ 5 MU 49 - MU 100	Yes	No	Update to SAFEQ 5 MU101 or newer Alternatively: SQ5-log4j-patcher tool
SAFEQ 6 Build 63 or older	Yes	Yes	Update to SAFEQ 6 Build 65 or newer Alternatively: Automated Log4jPatcher tool Alternatively: Automated Log4jPatcher tool in --update mode
SAFEQ 6 Build 64	Yes	No	Update to SAFEQ 6 Build 65 or newer Alternatively: Automated Log4jPatcher tool Alternatively: Automated Log4jPatcher tool in --update mode
SAFEQ 6 Build 65	No	No	N/A
SAFEQ Cloud	No	No	N/A – the installation already patched proactively by Y Soft
SAFEQ Managed	No	No	N/A – the installation already patched proactively by Y Soft
SafeQube 2	Yes	Yes	Update to SAFEQ 6 Build 65 or newer
Data Protection Tool included in SAFEQ 6 (all versions)	Yes	Yes	Update to SAFEQ 6 Build 65 or newer Alternatively: Automated Log4jPatcher tool
YSoft BE3D™ DeeControl 2	Yes	No	Update to SAFEQ 6 Build 66 or newer
YSoft SAFEQ Embedded Terminal	No	No	N/A – some Embedded Terminals are using Log4j, but they cannot be configured in a way to be vulnerable
YSoft BE3D™ DeeControl YSoft SAFEQ Client (SAFEQ 5 client) YSoft SAFEQ Client (SAFEQ 6 client) YSoft SAFEQ Client v3 YSoft SAFEQ Mobile Integration Gateway YSoft SAFEQ Mobile Print Server YSoft Card Reader Tool (and usbrtool.exe) YSoft IPP testing tool Mobile terminals Local Monitor	No	No	N/A – Java not used
YSoft SAFEQ Payment System Payment plugins for YSoft SAFEQ Payment System	No	No	N/A - Log4j not used
Customization provided by Y Soft	No	No	Extensions and other custom solutions provided by Y Soft do not directly use Log4j. However, there can be some third-party libraries that might theoretically use it. Should your security scan to reveal any potential security risks, please report it as an incident to Y Soft and we will update the affected extension with high priority.

Notes:

SAFEQ 6 Build 64 released on December 16 2021.

SAFEQ 6 Build 65 released on January 28 2022.

SAFEQ 6 Build 66 released on February 25 2022.

SAFEQ 5 MU 101 released on April 25 2022.

2.1 SAFEQ 6 - AUTOMATED LOG4JPATCHER TOOL

Download link (version 41) here

Usage instructions: see README.txt in the downloaded archive

Basic description:

- The tool scans the existing YSoft SAFEQ 6 and removes problematic *JndiLookup.class* from Log4j .jar files. This makes them invulnerable to CVE-2021-44228, CVE-2021-45046. This has no impact on any SAFEQ 6 functionality, it will work as intended without any limitations after applying the tool.
- Alternatively, the tool can update Log4j to version 2.17.2 to mitigate all the CVEs listed above since version 41 (--update option). This update mode should be run only with YSoft SAFEQ 6 MU30 up to YSoft SAFEQ 6 Build 64.

Recommendations:

- If you need to have the libraries update due to security tools detecting it, run version 41 with update option.
- If you previously used Log4jPatcher version 35 or older, also run version 40.
- If your security software still detects vulnerable log4j libraries or you want to eliminate all known vulnerabilities, run in --update mode.
- Check the hash of the .zip archive after downloading it:
  SHA1: F674CBDBDBB976EE825EF0FAE2689178816E895C
  SHA256: A384B2EA36FC20195A9114FCE5574F66F09F860533F2203F11BAD955CCB80182
- Check the .exe file digital signature before running it (signed by Y Soft).

2.2 SAFEQ 5 - SQ5-LOG4J-PATCHER TOOL

Download link (v5) here

Usage instructions: see USAGE.txt in the downloaded archive

Basic description: The tool is intended for YSoft SAFEQ 5 MU 49 - MU 100, it updates Log4j to version 2.17.2 to mitigate all the CVEs listed above. It cannot be used with YSoft SAFEQ 5 MU 48 or older because the new Log4j library requires JDK8+, which is available from MU 49. It cannot be used with SAFEQ 6.

Recommendations:

- Check the hash of the .zip archive after downloading it:
  SHA1: E398A4314387169FCB3B777F643D7B9651E278D8
  SHA256: 05E186299D239B1575C0B2CEEDBB17A2C72C9BF6D532ED0662D5749340D30B8F

2.3 FREQUENTLY ASKED QUESTIONS

Q: I used Log4jPatcher version 36 on my SAFEQ 6, do I need to run version 40 as well?
A: No, both versions provide the same, sufficient level of protection. While listening to feedback from people using the Log4Jpatcher tool, we made proactive improvements in language, verbose messages and the service startup order. Full details can be found in the tool README file. If you used version 35 or older, please run version 40 to mitigate the risks.

Q: Why is Y Soft releasing a new Log4j version in Build 65 when you claim that SAFEQ 6 Build 64 is fully secure?
A: Build 64 fixes vulnerabilities we consider CRITICAL by updating Log4j to version 2.16.0 (see Apache website for additional information). Build 65 updates Log4j to version 2.17.1 to also fix other vulnerabilities listed at the top of this page.

Q: I have SAFEQ 6 Build 64 or SAFEQ 6 Build 65 and a few files in " *<Management>\utilities\Import tool\lib* " are still flagged as vulnerable by Log4jPatcher. How is this possible?
A: Firstly, this will not happen for a new installation. However, if you updated from previous versions, those files might have been left there due to a defect in the update process (SBT-3494 - fixed in Build 66). The fastest solution is to run the following PowerShell script in the mentioned directory:

```
#Note: Running the script multiple times by mistake will cause no damage.
$list = 'log4j-api-*.jar','log4j-core-*.jar','log4j-jcl-*.jar','log4j-jul-*.jar','log4j-slf4j-impl-*.jar','spring-boot-starter-log4j2-*.jar'
ForEach ($tmp in $list) { gci *.* -Include $tmp | Sort { [decimal]($_.BaseName -Replace '\.RELEASE','' -Split ('\-|\.'))[-2] } | Select -SkipLast 1 | Remove-Item }
```

The script deletes all *log4j-*.jar* and *spring-boot-starter-log4j2-*.jar* from the mentioned directory except the ones having the highest number. The security impact is extremely low since the vulnerability can be only exploited at the time when the problematic class is loaded in the memory of a process, but the *import_tool.bat* that loads those jar files is not running constantly. It can be launched ad-hoc by a user with administrative rights on the server or by a scheduled task previously created by the administrator. For details about *import_tool.bat* usage, see the documentation of "*CLI Device Replicator*" or "*CLI User Replicator*".

Q: I used Log4jPatcher version 40 on SAFEQ 6, but my security software says SAFEQ is still vulnerable to CVE-2021-44228 (CRITICAL) or CVE-2021-45046 (CRITICAL). What should I do?
A: Some security tools report the vulnerability based on the version of log4j-core-*.jar instead of scanning for the vulnerable code. You can determine whether your installation is vulnerable by using our Log4JPatcher utility. Simply run " *Log4jPatcher.exe --dry-run* ". When there are no vulnerable files reported,

SAFEQ is not vulnerable and the detection is false positive. In Build 65, Log4j is updated to 2.17.1, which fixes the most recent vulnerabilities and even the scanners relying on the filename/version will stop reporting the vulnerability. Starting with version 41 of our Log4JPatcher utility, the --update mode should also remove all occurrences of those false positives because all log4j libraries are updated to 2.17.2.

Q: What should I do if I have a SAFEQ that is affected by a vulnerability you consider non-critical? (CVE-2017-5645, CVE-2019-17571, CVE-2020-9488, CVE-2021-4104, CVE-2021-44832, CVE-2021-45105)
A: You are not in a direct danger. Please refer to the explanation about CRITICAL and NOT CRITICAL vulnerabilities at the top of the article. When possible, update to the SAFEQ version containing the latest Log4j, as defined in the table at the top of the page. Alternatively, you could remove the following classes to remove the vulnerable code and restart all YSoft SafeQ services on the server where removal was performed (but as mentioned, we do not feel this is necessary):
SAFEQ 4 - *JMSAppender.class , SocketServer.class , SMTPAppender.class, SMTPAppender$1.class* from *log4j-*.jar*
SAFEQ 5 - *JMSAppender.class , SocketServer.class , SMTPAppender.class, SMTPAppender$1.class* from *log4j-*.jar*
SAFEQ 6 - *JMSAppender.class , SocketServer.class , SMTPAppender.class, SMTPAppender$1.class, JdbcAppender.class* from *log4j-core-*.jar* (this jar is also inside the *<Management>\tomcat\webapps\ROOT.war*)
YSoft BE3D™ DeeControl 2 - JMSAppender.class, JdbcAppender.class, JndiLookup.class from **.jar* (within DeeControl 2 install dir or subdirs, it is necessary to quit the application before modifying *.jar)

Q: Initially, SAFEQ 6 required manual reconfiguration to mitigate CRITICAL vulnerabilities. Is this still necessary?
A: No, manual reconfiguration is not necessary. Either update to Build 64 and newer or use the Log4JPatcher tool. The aim of the initial advisory was to provide a quick response at the cost of time-consuming manual steps. Since then, we have worked hard and provided convenient and automated protection for our customers.

Q: I cannot access Management Interface after applying Log4jPatcher. How can I fix it?
A: In rare cases, this may happen. But there is a very simple solution in deleting the temporary files of a web server:

- Stop "YSoft SafeQ Management Service"
- Delete the repository <SafeQ6>\Management\tomcat\webapps\ROOT
- Start "YSoft SafeQ Management Service"

- Verify the situation is resolved

Q: How exactly is SAFEQ 5 MU 101 mitigating the mentioned CVEs?

A: It updates Log4j to version 2.17.1, which is not vulnerable.

Q: Why do I have to update YSoft BE3D™ DeeControl 2 to Build 66 or newer?

A: YSoft BE3D™ DeeControl 2 uses log4j version 2.17.1, starting from Build 66. This Log4j version mitigates all the mentioned CVEs.

Q: You are saying that YSoft BE3D™ DeeControl 2 is not vulnerable to CRITICAL vulnerabilities. But its .jar files contain *JndiLookup.class* , which is related to CVE-2021-44228 (CRITICAL) and CVE-2021-45046 (CRITICAL). Can you explain that?

A: YSoft BE3D™ DeeControl 2 is commonly run on workstations by users without administrative privileges. The attack against Log4j within the application could be only conveyed by the person running its process, which would not result in any higher privilege gains. In addition, the application is not accepting any remote commands, which minimizes the risks – and even if it was, it is only running ad-hoc as a process (it is not a service that would be running constantly) and this greatly reduces risks by shortening the time window for the possible attack.