YSOFT SAFEQ LOG4J VULNERABILITY MITIGATION
December 20, 2021

Introduction

Y Soft is closely monitoring the evolving situation around the Apache log4j vulnerabilities and providing up-to-date security advisory whenever the situation develops.

This 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. Three vulnerabilities have been reported and tracked as CVE-2021-44228 (nist.gov), CVE-2021-45046 (nist.gov), and CVE-2021-45105 (nist.gov). Apache has acknowledged these vulnerabilities and has released patched versions 2.15 and 2.16, with 2.17 to follow anytime soon.

YSOFT SAFEQ6 Release 65 (due January 31) will be released with the most up-to-date log4j version available.

How does this affect YSOFT SAFEQ?

The following versions of SAFEQ are fully patched:

- YSOFT SAFEQ6 build 64
- YSOFT SAFEQ6 Managed build 64
- YSOFT SAFEQ Cloud

Customers using YSOFT SAFEQ Cloud and YSOFT SAFEQ Managed do not have to do anything as their installations are already patched proactively by Y Soft.

Y SOFT SAFEQ versions **prior to Build 64** require the following mitigation steps

SAFEQ Version	Vulnerable	Mitigation
SAFEQ 4	No	Not required
SAFEQ 5	No	Not required. See FAQs
SAFEQ 6 B1 up to B63	Yes	**Preferred**: Upgrade to SafeQ Build 64 **Alternatively**: Automated Log4jPatcher tool
SAFEQ 6 B64	No	Released December 16. Fully Patched
Data Protection Tool included in SAFEQ 6 (all versions)	Yes	**Preferred**: Upgrade to SafeQ Build 64 **Alternatively**: Automated Log4jPatcher tool

Steps to apply the Automated Log4jPatcher tool

To mitigate the CVE-2021-44228 and CVE-2021-45046 vulnerabilities, we have released the Log4jPatcher tool. This tool replaces the **workaround steps published on December 13, 2021**, for CVE-2021-44228 and extends the mitigation by including the CVE-2021-45046 mitigation**. Customers who used the workaround steps are advised to run the patch tool** to be fully protected.

The Automated Log4jPatcher tool was released on December 14, 2021 (version 36) to cover CVE-2021-44228. **Customers who used this version are advised to download and run the latest version (version 40)** release to mitigate CVE-2021-45046.

This tool scans your existing YSoft SAFEQ 6 and fixes all occurrences of the affected log4j library. It removes the vulnerable code from each library and adjusts the runtime configuration to SAFEQ to disable the attack vector of the vulnerability. Please note that this has no impact on any SAFEQ 6 functionality. Your SAFEQ 6 installation will work as intended without any limitations after applying the tool.

You can download version 40 of the tool in a .zip archive with a short README document from here. The binary file (exe) is digitally signed by Y Soft. Please make sure that the file is correctly signed before running it. To confirm that you are using the right file, here are the hashes of the .zip archive.

SHA1: 21AE0CA4B52F49AF2FB80AD87E645BB7438CC6E1
SHA256: 6A0C9A4D98CB5A618D0F7B69886EB2DE481705D6072651DA47F5FBEA2F7684CC

Upon completion of the Log4jPatcher tool, confirm that all YSoft Windows Services are running. At this point, the patch has been successfully applied.

Frequently Asked Questions

How does Y Soft address the most recent vulnerability: CVE-2021-45105?

YSoft SAFEQ 6, SAFEQ 5, and SAFEQ Cloud do not suffer from this vulnerability as we are not using the affected features in our products. Specifically, we do not use user inputs in contextual logging messages.

My anti-virus software has indicated that SAFEQ is vulnerable even with SAFEQ 5 or after running the Log4jPatcher. What should I do?

Some anti-virus tools are not properly checking the log4j library versions and are simply testing for log4j-core-*.jar file instead of scanning for the vulnerable code. You can determine whether your installation is vulnerable by using our Log4JPatcher utility.

```
Log4JPatcher.exe --dry-run
```

This will produce a list of log4j libraries that still contain vulnerable content. On patched installations, the list will be empty.

Why is Y Soft releasing a new log4j version in build 65 when you claim that SAFEQ 6 build 64 is fully secure?

Customers are required to apply patch to SAFEQ 6 build 63 and older. Our aim with build 64 and the upcoming 65 (January) has been to provide a fully secure, up-to-date installation package that does not require any additional actions from customers or partners. In other words, to make the securing process more convenient for you.

Y Soft originally announced that SAFEQ 5 is not vulnerable because of using log4j 1.x. This library is now indicated as vulnerable. Is SAFEQ 5 safe or not?

The vulnerability in log4j v1.x is related to JMSAppender code, which enables logging into Java Messaging Service-compliant system. YSoft SAFEQ is not using such a configuration by default and does not support such a configuration for our customers.

Initially, YSoft SAFEQ required manual reconfiguration to mitigate the vulnerabilities. Is this still necessary?

No. Either update to build 64 or use the Log4JPatcher tool. No manual reconfiguration is necessary. The initial advisory has been released to provide a quick response at the cost of requiring manual steps. Since then, we have worked hard and have provided convenient and automated protection for our customers.

Why is Y Soft releasing newer versions of the Log4JPatcher tool?

The core functionality of the tool remains the same. All versions provide the same, sufficient level of protection. We are listening to feedback from people using the Log4Jpatcher tool and are making proactive improvements.

Version 40 of the Log4jpatcher tool includes:

- an improved README file based on feedback
- added logging (log file is created)
- an added verification before stopping/starting NRG services
- reduced default verbosity of the output
- a new --verbose switch that enables verbose logging
- a new banner to mark the log visibly when running in dry run mode
- better error handling for broken jar or war files (they will be skipped)
- a fix for the path argument (previously, the path stored in the Windows registry always overrode the value of the argument)