Australian Government
Australian Digital Health Agency

Request for Information – Widespread critical vulnerabilities Digital Health Cyber Security

31 May 2022 v1.0
Approved for external use
Document ID: SEC-310522-01

What has happened?

Recently two critical vulnerabilities in software libraries have created vulnerabilities in many of the applications and devices that incorporate those software libraries. The Australian Cyber Security Centre (ACSC) issued alerts about :

- a critical vulnerability in the widely used **Apache Log4j2 library** in December 2021. Exploitation of this vulnerability could allow cyber criminals access to your or your customers' networks. It has the potential to disrupt business operations, loss of business and recovery costs, including reputational damage and regulatory action. [1] Exploitation of the Log4j2 library began on or around 1 December 2021, and a proof-of-concept exploit is publicly available. [2]
- a critical vulnerability in the widely used **Spring Framework library** in March 2022**.** The Spring Framework is a popular Java development framework used to build a broad range of software, including web applications and APIs. Spring4Shell (CVE-2022-22965) is a remote code execution vulnerability [3], which impacts the Spring Framework with Java Development Kit (JDK) version 9.0 or higher. According to some sources, [4] the vulnerability can be exploited regardless of the application server. [4] [5] Proof-of-concept exploits are publicly available.

The Log4j2 and Spring Framework are used broadly in a variety of consumer and enterprise web applications and devices, including some operational technology products. [6]

Purpose

The Australian Digital Health Agency (the Agency) would like to know if these vulnerabilities affect *the health software developed by your company*.

If so, the Agency recommends that your company provides advice *publicly,* for the benefit of your customers and other relying parties.

Disclosing vulnerability information in software applications and devices *publicly*, is generally better than private disclosure because it leads to more rapid and complete mitigations and helps builds confidence in the vendor's security processes for relying parties, including the vendor's customers. Therefore, the Agency recommends that you publish advice *publicly*, as to whether your company's software products are affected by these vulnerabilities; the patches available, and any mitigation actions that need to be taken.

Request for information

Given the criticality, and widely dispersed nature, of the Log4j and the Spring Framework vulnerabilities, the Agency, as the System Operator for the My Health Record system, is writing to software developer organisations and hosted service providers which are authorised to connect to the My Health Record system. This includes:

- conformant software vendors
- repository operators and portal operators
- hosted service providers and contracted service providers
- Agency contracted software vendors and hosted service providers

As one of these stakeholder groups, we request that your organisation/company informs us whether your software products or hosted services contain the component software libraries with the Log4j2 and/or Spring Framework vulnerabilities; and if so whether these have been mitigated. [6] [7]

Complete the questionnaire

We request that, within 14 days of this email's sent date, you inform us if your products or services currently have any of the Log4j2 or Spring Framework vulnerabilities.

Please do this by completing the short questionnaire: https://surveys.digitalhealth.gov.au/n/2DKc1p4 .

The vulnerabilities

The vulnerabilities are summarised below:

CVE	CVSSv3	Publication date	Reference
CVE-2021-44228 (aka Log4Shell) Apache Log4j2 2.0-beta9 through 2.15.0	Critical 10	10 Dec 2021	https://nvd.nist.gov/vuln/detail/CVE-2021-44228
CVE-2021-45046 Apache Log4j 2.15.0	Critical 9.0	14 Dec 2021	https://nvd.nist.gov/vuln/detail/CVE-2021-45046
CVE-2021-4104 JMSAppender in Log4j 1.2	High 7.5	29 Dec 2021	https://nvd.nist.gov/vuln/detail/CVE-2021-4104
CVE-2022-22965 (aka Spring4Shell) Spring Framework	Critical 9.8	31 March 2022	https://nvd.nist.gov/vuln/detail/CVE-2022-22965

Mitigation

Log4j2

The ACSC has published Log4j2 mitigation advice for ICT teams; [1] [2] advice about how to manage supply chain risks; [8] and advice that boards and company directors need to know and should be asking their ICT teams about this vulnerability. [9]

Spring Framework

Organisations should consult and action the recommendations contained within the vendor's security advisories relating to CVE-2022-22965. The best way to fix Spring4Shell is to upgrade the Spring Framework to version 5.2.20 or 5.3.18. If you are using Spring Boot directly, then upgrade to version 2.6.6. [3] [10] Some experts advise patching even if you are not using Tomcat as an application server. [4]

The resources below list vendor products with the vulnerabilities:

- CISA's Github repository [6]
- National Cyber Security Centre – Netherlands (NCSC-NL) [11]

Our role

The statutory functions of the Agency include developing, implementing, managing, operating, and continuously innovating and improving standards, systems, and services to deliver nationally consistent and interoperable digital health capability for Australians.

A priority for the Agency is to enable transparent and sustainable governance of digital health standards. This involves collaborating with industry, governments, healthcare representatives and consumers about these standards. The standards will create the foundations for software conformance to build quality and enable the greatest benefits from digital health for healthcare providers and all Australians.

As the System Operator for the My Health Record system, the Agency is also responsible for protecting the integrity and security of the My Health Record system. Our request for information relates to the Agency's role to protect the My Health Record system and associated national infrastructure; and reflects our expectation that conformant software vendors, hosted service providers, and repository and portal operators should routinely report publicly about security vulnerabilities in their software products or hosted services.

Contact us

If you have any questions, please send an email to help@digitalhealth.gov.au

References

1. Australian Cyber Security Centre. *2021-007: Apache Log4j2 vulnerability – advice and mitigations*. Available from: https://www.cyber.gov.au/acsc/view-all-content/advisories/2021-007-apache-log4j2-vulnerability-advice-and-mitigations.
2. Australian Cyber Security Centre. *Mitigating Log4Shell and Other Log4j-Related Vulnerabilities*. Available from: https://www.cyber.gov.au/acsc/view-all-content/advisories/mitigating-log4shell-and-other-log4j-related-vulnerabilities.
3. Spring Blog. *Spring Framework RCE, Early Announcement*. Available from: https://spring.io/blog/2022/03/31/spring-framework-rce-early-announcement.
4. JFrog. *SpringShell (Spring4Shell) Zero-Day Vulnerability CVE-2022-22965 : All You Need To Know*. Available from: https://jfrog.com/blog/springshell-zero-day-vulnerability-all-you-need-to-know/.
5. Australan Cyber Security Centre. *Multiple vulnerabilities present in the Spring Framework for Java*. Available from: https://www.cyber.gov.au/acsc/view-all-content/alerts/multiple-vulnerabilities-present-spring-framework-java.
6. Cybersecurity & Infrastructure Agency. *CISA Log4j (CVE-2021-44228) Vulnerability Guidance*. Available from: https://github.com/cisagov/log4j-affected-db.
7. Cybersecurity & Infrastructure Agency. *Apache Log4j Vulnerability Guidance*. Available from: https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance.
8. Australian Cyber Security Centre. *Cyber Supply Chain Guidance*. Available from: https://www.cyber.gov.au/acsc/government/cyber-supply-chain-guidance.
9. Australian Cyber Security Centre. *Log4j: What Boards and Directors Need to Know*. Available from: https://www.cyber.gov.au/acsc/view-all-content/publications/log4j-what-boards-and-directors-need-know.
10. NIST. *CVE-2022-22965 Detail*. Available from: https://nvd.nist.gov/vuln/detail/CVE-2022-22965.
11. NCSC-NL. *Overview of software (un)affected by vulnerability*. Available from: https://github.com/NCSC-NL/spring4shell/blob/main/software/README.md.

Publication date: 31 May 2022

Australian Digital Health Agency ABN 84 425 496 912, Level 25, 175 Liverpool Street, Sydney, NSW 2000 digitalhealth.gov.au
Telephone 1300 901 001 or email help@digitalhealth.gov.au

Disclaimer
The Australian Digital Health Agency ("the Agency") makes the information and other material ("Information") in this document available in good faith but without any representation or warranty as to its accuracy or completeness. The Agency cannot accept any responsibility for the consequences of any use of the Information. As the Information is of a general nature only, it is up to any person using or relying on the Information to ensure that it is accurate, complete and suitable for the circumstances of its use.

Document control
This document is maintained in electronic form and is uncontrolled in printed form. It is the responsibility of the user to verify that this copy is the latest revision.

OFFICIAL

Acknowledgements
The Australian Digital Health Agency is jointly funded by the Australian Government and all state and territory governments.