Safety Action Notice

Reference **SAN2202** Issued **12 January 2022** Review Date **12 January 2023**

Medical devices and cybersecurity: LOG4J2 Vulnerabilities (CVE-2021-44228)

Summary

Several security vulnerabilities have been identified which affects a wide range of IT systems making them vulnerable to attack. Medical devices connected to networks and their supporting systems are also vulnerable which means their safety and performance may be adversely affected.

Action

1. This notice should be brought to the attention of all appropriate managers and staff.

2. A co-ordinated action plan should be developed with input from medical device and cybersecurity leads.

3. Action plans should include the following:
   - Identify all network connected medical devices and their supporting systems in asset registers that may use Apache Log4j2 versions.
   - Contact the respective manufacturers and suppliers for further information and support in identifying and mitigating the risks from the ‘log4shell’ security flaw.
   - Run and execute available scanning tools to identify the ‘log4shell’ vulnerability that may be present. Report any issues identified by the software scan to manufacturer as well as your local IT security team and Incident Reporting & Investigation Centre (IRIC).

Background

On Friday 10 December 2021, a critical security vulnerability was publicly disclosed affecting a wide range of business and web applications. Known as ‘log4shell’, this vulnerability allows remote code execution without authentication, i.e. without username and password. Since the initial disclosure, additional vulnerabilities have been identified and disclosed.

Log4shell is a systemic vulnerability, but it also affects a wide range of medical devices which connect to networks as well as their supporting systems. Scottish Government Cyber Resilience Unit has issued a communication providing information and guidance (Scotland Public Sector wide) and so has NSS (for NHS Scotland). This alert is not intended to duplicate these communications but to ensure there is co-ordination between medical devices and cybersecurity departments.

Depending on the nature of exploitation, the Log4shell vulnerability may result in the safety and functionality of medical devices being adversely affected.

- Vulnerability CVE numbers:
    1. CVE-2021-44228 | CVSS Score: 10 (Critical)
    2. CVE-2021-45046 | CVSS Score: 9 (Critical)
    3. CVE-2021-45105 | CVSS Score: 5.9 (Medium)
    4. CVE-2021-44832 | CVSS Score: 6.6 (Medium)

- Additional technical information on the vulnerabilities is available at:
    1. https://www.ncsc.gov.uk/news/apache-log4j-vulnerability
    2. https://logging.apache.org/log4j/2.x/security.html
    3. https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

MHRA is aware of the Log4j2 vulnerabilities and may produce additional communication.

Suggested onward distribution

Healthcare	Corporate and Support	Social Care
Ambulance Services	Device Managers	Care homes
Blood Transfusion	Health & Safety	Facilities management
Dental Hospitals	IT/Computing	Health, safety and wellbeing
General Dental Practitioners	Medical Physics	Home Care services
General Medical Practitioners	Risk Management	HSCP Chief Officer
Health Centres	Supplies/Procurement	Loaned equipment stores
Hospices		Special schools

Enquiries

Enquiries and adverse incident reports should be addressed to:

Incident Reporting & Investigation Centre (IRIC)
NHS National Services Scotland
Gyle Square, 1 South Gyle Crescent, Edinburgh EH12 9EB
Tel: 0131 275 7575 Email: nss.iric@nhs.scot

For information on how to report an incident: How to report an Adverse Incident

General information about adverse incidents and safety alerts can be found in CEL 43 (2009) or by contacting IRIC at the above address.

Annexe

Cyber Security
A NSS Centre of Excellence

NHS National Services Scotland

cyberQuarter, Dundee
csoc@nhs.scot

EXECUTIVE BRIEFING: 'LOG4J2' VULNERABILITY (CVE-2021-44228)

EXECUTIVE SUMMARY

A new **critical and systemic** vulnerability affecting a wide range of systems has been identified and is being actively exploited by attackers. This vulnerability, known as **'log4shell'** allows attackers to remotely run their own code on systems from anywhere on the network (or Internet if the application is Internet facing) without a username or password.

Attempts to exploit this vulnerability are ongoing, due to the ease with which they can be carried out.

All NHS Organisations are asked to be aware and check for the presence of this vulnerability in their systems and in the systems of services provided to them by third parties and to patch those systems accordingly. The CCoE is working on a package of mitigating advice and guidance and collaborating with national critical suppliers on the issue and further, technical, briefings will be made available to infrastructure and information security leads.

BACKGROUND

On Friday 10 December 2021, a critical vulnerability was reported affecting a wide range of business and web applications that use several Apache Log4j2 versions. Known as 'log4shell' and assigned CVE-2021-44228, this is a logging-related vulnerability that allows remote code execution without authentication (i.e., without username and password).

The bug affects a Java package called log4j - a library that helps IT administrators create logs - and is already being exploited in the wild by a range of threat actors. Attackers who can control log messages or log message parameters can execute their own unauthorised code, which could be used to steal data from affected systems, modify the behaviour of those systems, or affect their functionality.

This is a *systemic* vulnerability due to the prevalence of log4j in modern IT environments. All Health Boards and Managed Service Providers could be affected. **NSS Intrusion Prevention Systems (IPS) have already identified and are blocking attempted exploitation.**

Attackers have been observed utilising multiple techniques to exploit the vulnerability including: entering malicious code into username/password fields, renaming twitter accounts, renaming iPhones, posting messages on chat boards and adding malicious code to HTTP headers.

Many advisories, vendor patches and mitigating rules for security appliances are being created and published in the aftermath of the vulnerability being disclosed. The CCoE are working through these to provide best advice and guidance for NHS Scotland Health and Social Care organisations.

ANALYSIS

This is a complex situation, not least because of the nature of the package within which the vulnerability has been discovered. Within hours of being notified, Apache, one of the key vendors with widespread

Annexe (continued)

exposure, issued a new version for application developers. Other major systems providers, including Oracle, have also distributed the patch. However, developers must now push out updates for their applications, which may give more time for exploitation by attackers. In the immediate term, IT and Infrastructure Teams will need to rely on advice from application providers to apply mitigations.

This vulnerability is classed as very easy to exploit, exacerbating its seriousness. It also comes at a time when the NHS is ramping up digital services to meet the increased demand for Covid boosters in the face of the Omicron variant. Our assessment is that the most likely motives for carrying out an exploit against NHSS systems are:

- Security researchers scanning for vulnerable systems
- Cryptocurrency mining
- Botnet acquisition (adding our systems to compromised networks under an attacker's control)
- Data theft
- Ransomware or other malware deployment

It will likely take several weeks and months for all organisations and cloud providers to fully patch their applications. The sheer range of systems in which the vulnerability will be present makes this a marathon and not a sprint. Nevertheless, immediate priority and urgency should be to follow the recommendations in this paper.

ACTIONS TAKEN BY CYBER CENTRE OF EXCELLENCE

The CCoE via NSS Digital and Security is working with national systems providers to provide assurance that they are aware of and remediating the vulnerability. There is a raft of technical information and advisory material being published regarding this vulnerability and this is being evaluated for publication of consolidated advice and guidance. We are also in liaison with the Digital Health & Care Department (Competent Authority) and the Scottish Government Cyber Resilience Unit to consolidate advice and guidance and provide same where possible to other organisations.

RECOMMENDATIONS

There are three activities that NHS Scotland and Social Care organisations should seek to answer as a priority:

- Search for and identify all systems and supporting infrastructure that are vulnerable; priority should be given to *externally facing internet connected systems*.
  - Identify software applications in use that that includes log4j2. Software written in Java often uses log4j.
- Patch vulnerable systems as soon as patches become available from vendors and in line with critical patching policies.
- If immediate patching is not possible, consider implementing the following:
  - Configure Log4j as per Apache's advisory (https://logging.apache.org/log4j/2.x/security.html)
  - Configure host and network firewalls to block inbound exploitation attempts
  - Configure intrusion prevention systems to block attempts
  - Configure web application firewalls to block attempts
  - Restrict outbound network connections for vulnerable systems

It is requested that the results of these actions are communicated to the CCoE so that we can determine and report on the national security posture in relation to this vulnerability.

Should organisations require further assistance or guidance, please contact the CCOE using the established Security Teams channel, or via csoc@nhs.scot and we will endeavour to help.