Board update

Subject:	Log4J Vulnerability	**Date:**	3rd March 2022
Prepared By:	Jacqueline Widdowson, IG Manager/DPO SFH, **Contributors:** James Beresford, Head of Technical Delivery, NHIS, Richard Melanaphy, Head of Governance and Assurance NHIS , Mark Stone, Emergency Planning SFH.		
Approved By:	David Selwyn		
Presented By:	David Selwyn		

Purpose		
To inform and provide assurance to the Board in relation to the guidance issued by the UK National Cyber Security Centre, which outlines 10 key questions that boards should review and ask their IT teams.	**Approval**	
	Assurance	**X**
	Update	
	Consider	

Strategic Objectives				
To provide outstanding care	**To promote and support health and wellbeing**	**To maximise the potential of our workforce**	**To continuously learn and improve**	**To achieve better value**
	x	**x**	**x**	**x**

Overall Level of Assurance				
	Significant	**Sufficient**	**Limited**	**None**
		x		

Risks/Issues	
Financial	**Non-compliant with legislation could lead the Trust into incurring fines from the ICO and reputational damage**
Patient Impact	
Staff Impact	
Services	
Reputational	

Committees/groups where this item has been presented before

None

Executive Summary

Log4J is a worldwide, pan-industry, popular software utility in Java applications/software.

A vulnerability called Log4shell was identified in particular versions of this software and on 10th December 2021, the UK National Cyber Security Centre issued a High Security Alert and then on 11th December 2021 the Government Security Group initiated work across government and sectoral cyber teams to clarify potential risks and possible exposure.

Over the weekend of 11th December a team within Nottinghamshire Health Informatics Service (NHIS) was mobilised to commence work on mitigations with respect to this threat and this work continues to date.

The UK National Cyber Security Centre have issued 10 key questions that Trust Boards should ask IT departments.

Provided below is a response to those 10 key questions, which includes details of who is leading the response for the Trust, the individuals involved and the support to these teams.

Details of the Log4J management plan is also included, along with the tools being used to mitigate the risk of a Log4J security penetration.

Business Continuity Plans (BCP's) and incident response plans are in the process of being updated for the Trust and this will be monitored via the Information Governance Committee and any items of escalation forwarded to the Risk Committee.

Further explanation is provided by the National Cyber Security Centre here;
Log4j critical vulnerability advice for boards - NCSC.GOV.UK

Trust Board are asked to;

- note the contents of the report and the assurance provided

Log4J Vulnerability 10 Key Questions to IT Teams

Who is leading the response?

An NHIS team was stood up in response to the Log4j vulnerability due to the vulnerability being classed as a V2C (Vulnerability at Level 2 for Critical Public Infrastructure).

The designated NHIS lead is the Head of Technical Delivery, with responsibility for updating the High Severity Alert (HSA) status on the National Cyber Portal.

Updates on progress of the Log4J vulnerability plan are reported through the NHIS Cyber Security Assurance Programme Board, which includes the respective SIRO's for each organisation. Assurance in relation to the trust actions and progress is reported through the Information Governance Committee.

The Head of Technical Delivery attends the regular National Cyber briefings in relation to Log4j to ensure any new intelligence gathered is shared across the respective teams and organisations.

What is our plan?

A risk-based approach was devised, focusing on the higher risk areas first.

The initial response was to close down access to any published resources to external networks (Internet & Health and Social Care Network - HSCN).

Because Log4j is extensively used and frequently embedded in pieces of software, equipment and hardware, the focus was to contact suppliers of the larger strategic software components and infrastructure to receive verification about the use of particular versions of Log4j. Any mitigations or remediations (upgrades or patches) have been applied as required.

Pro-active scanning has also been conducted, internally and externally via vulnerability and security posture tools, with specific log4j signatures and policies for assurance before re-publishing services back to the external networks.

All tools used have had additional Log4j scanning or reporting capabilities added by the respective vendors and NHIS continue to utilise these for monitoring log4j vulnerable software or and as identified, work with vendors and customers to specifically remediate identified software across the estate.

How will we know if we're being attacked and can we respond?

From a server and desktop perspective, Endpoint Detection and Response tools have been updated with Log4j monitoring and reporting. Anti-Virus/Anti-Malware software has the added ability to scan for Log4j activity. To date, neither tool has reported any Log4j malicious activity, and no Log4j Indicators of Compromise (IOC) have been detected.

From a network boundary perspective, firewalls are in place at each site, at the Data Centre Boundary and at network egress points. All firewalls are configured to log and block and Log4j attempts with activity logs being monitored regularly.

NHS Digital provide an additional external layer of protection on the HSCN network known as Secure Boundary, which they utilise to monitor and report on any suspected Log4j activity.

Although the vulnerability has been exploited in some industries world-wide, to date, there are still no known exploits in the NHS.

What percentage visibility of our software/servers do we have?

NHIS have full visibility of all desktops, servers and the software instances installed across the estate for any corporate device connected to the NHS local networks. Reports are available from the Endpoint Detection and Response platform, and also from 3rd party assurance tools. There is however a need to seek assurance from suppliers of software and hardware due to Log4j being deeply embedded and therefore not necessarily detectable and this is on-going work.

How are we addressing shadow IT/appliances?

Early in the Log4j vulnerability the NHIS team arranged a briefing with the Cyber Security Assurance Programme Board to outline the risks associated with the Log4j vulnerability, the response NHIS were taking and the required response from all organisations. This included the requirement for organisations through their Information Asset Owners to make contact with all suppliers and services that are utilised to obtain assurance of whether or not Log4j is utilised and any required mitigations. Examples of assets include specialist hardware e.g., MRI scanner, cloud-based applications, and specific clinical system contracts e.g. Medway.

Do we know if key providers are covering themselves?

Suppliers are being contacted and as part of the engagement a centrally shared spreadsheet on a secure site has been created to log all supplier response activity and status. This is shared across the NHIS partner and customer organisations to allow an overview of the suppliers and assets in situ, when they were contacted and what the status of the Log4j vulnerability. The IG team continue to engage with IAO's to ensure suppliers are contacted and responses are received.

Does anyone in our organisation develop Java code ?

NHIS have confirmed Java is not currently used as part of Development Services. Locally developed applications that have used Java historically have been assessed for the use of Log4j.

How will people report issues they find to us?

A central mailbox has been created for collating supplier responses. Technical staff are monitoring the responses and ensuring remedial action is taken where required. NHS Digital are also reporting known vulnerabilities they are made aware of through the High Severity Alerts (HSA's) for acting on. Responses to these HSA's are reported through the National Cyber Portal.

When did we last check our business continuity plans (BCP) and crisis response?

Business Continuity Plans exist for all areas of the trust and are tested on an annual basis with the last test being 30th June 2021.

NHIS is currently reviewing Business Continuity and Incident Response Plans and, as part of this process, has presented the most recent version at Strategic Leadership Group (SLG) for observations prior to acceptance and ratification. A workshop to establish the correct way to recognise and escalate an event to Business Continuity Response status is being planned with the Chief Technical Officer and this work will be reported on at SLG. NHIS is working with Partners and the Emergency Planning Officer to deliver a business continuity exercise, rehearsing plans and identifying learning points – and supporting Data Security & Protection Toolkit submissions by organisations – prior to March 2022.

How are we preventing teams from burning out?

Rotation of the relevant technical discipline resources occurred with other members of the team to ensure rest and recovery, whilst the team could still engage with the incident. Initially the team met daily to share updates, plan the response and allow regular reporting. As per NHSD guidance that 'this is a marathon, not a sprint' is important as we manage this as a long-term activity.

Dedicated communication channels for HSA alerting and updates are in place; and the NHIS team have established a bi-weekly comms cell to discuss Log4j and other related HSA alert activities. Updates are being provided through the Information Governance Groups.

Going Forward

Regular updates will be provided to the Information Governance Committee and any items of escalations forwarded to the Risk Committee. Updates are also being provided to the Cyber Security Assurance Programme Board.