Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Log4j: What Boards and Directors Need to Know

What is Log4j, and the Log4j Vulnerability?

Log4j is a software library used as a building block found in a wide variety of **Java** applications. It provides logging functionality in many products ranging from messaging and productivity applications, mobile device managers, teleconference software, web hosting and even video games. **Over 100,000 products from hundreds of vendors – and in house developed software – may contain Log4j.**

The Log4j vulnerability – otherwise known as Log4Shell – is trivial to exploit, and represents a significant business continuity risk. Successful exploitation can lead to system and network compromise. **If left unfixed malicious cyber actors can gain control of vulnerable systems; steal personal data, passwords and intellectual property; and install malware such as backdoors for future access, cryptocurrency mining tools and ransomware.**

Why should boards be concerned?

The Log4j vulnerability is a serious business continuity risk. If exploited by malicious actors, the vulnerability has the potential to significantly disrupt your business operations, incur significant incident response costs, damage your organisation's brand and reputation, and depending on the response of the Board, may be a cause of shareholder or regulatory action.

A large number of Australian organisations use products or services which use the Log4j library. Due to its widespread use in popular software and hardware platforms a large number of third-party applications may also be vulnerable to exploitation through this vulnerability. **Many Australian organisations develop software or hardware with embedded software – either internally or as a product for customers – which include the Log4j library.**

Australian organisations are being targeted and compromised. The ACSC is aware of widespread targeting of Australian organisations by malicious actors to identify the Log4j vulnerability. The ACSC has observed successful exploitation of the Log4j vulnerability and the compromise of systems and networks within Australia and globally, across all sectors of the economy.

The vulnerability is easily exploited across the internet. Internet facing systems – such as your web stores and other websites or services used by customers – are most at risk of compromise and disruption. Other systems that support business activities, such as video conferencing or remote access solutions may also be impacted and could provide further opportunities for malicious cyber actors to compromise internal networks or cloud environments.

Managing this risk requires strong leadership from the Board working in concert with executives and technical teams to understand an organisations exposure and take actions as appropriate to individual organisations. Encouraging an organisational design and culture that supports cybersecurity is important, and supporting technical experts and IT departments is essential.

What questions should boards be asking?

In the context of Log4j and the increasing prevalence of cyber attacks, it is important your board have measures in place to respond to cyber security incidents when required. Consider discussing these questions as a board, with your executive team and with internal IT managers, or outsourced service providers to ensure you are equipped with the most relevant information.

What are the organisation's and the board's obligations?

Understanding and managing cyber security risk within the organisation, as with any other business risk, is a **key responsibility to protect the company and its shareholders** and an important aspect of fulfilling your duties and obligations as directors. The board should seek to understand as much as possible about cyber security risks with a view to understanding what information technology systems are critical for the organisation's core business, how they could be exposed to cyber threats and what mitigations are in place to control risks to those systems.

If your organisation produces or distributes Java based software, your organisation has a responsibility to identify whether Log4j is used in your products or to offer services to customers. Your organisation may have legal and contractual obligations to urgently develop patches for your products and assist your customers implement mitigations to reduce the likelihood of harm from the Log4j vulnerability.

The board may have regulatory obligations such as those under the *Privacy Act 1988* and *the Notifiable Data Breach Scheme* which requires all businesses covered by the *Australian Privacy Act 1988* to notify the OAIC and affected individuals when an eligible data breach has occurred. If you have identified a breach, it is important that your communication is transparent, honest and timely.

There are significant time pressures for decision making when responding to a cyber security incident. **As a board, you should ensure you are available and prepared to make critical decisions that might exceed the delegated authority of executives and update your organisation risk appetite statement as required by a dynamic situation.**

How are the Board and management team staying informed?

It is crucial that directors, and executives, seek out the most accurate and timely information from reputable sources. Look within your organisation to your experts including the Chief Information Officer (CIO), Chief Information Security Officer (CISO) or IT Managers.

Consult reputable sources of information on the changing threat environment including the Australian Cyber Security Centre (ACSC), the UK National Cyber Security Centre (NCSC) and the US Cybersecurity and Infrastructure Security Agency (CISA).

Boards should ask CIOs or CISOs whether your organisation has joined the ACSC Partnership Program. Being a partner ensures that you have the most up to date ACSC information including sensitive reporting from the ACSC. Details are available on cyber.gov.au at https://www.cyber.gov.au/resources-business-and-government/become-acsc-partner.

Boards should also ensure that CIOs, CISOs or IT Managers are up to date with the **latest patching and mitigation advice from key vendors and service providers**.

As always, boards through their Audit and Risk Committees should conduct period audits of cyber security, and embed regular updates on cyber incidents, trends and risks as part of your audit and risk governance.

Who is leading on our response?

It is important to have one person in charge of the response to Log4j, and any arising cyber security incidents, to ensure clarity and timely decisions on operational requirements, prioritisation, continuity and communications.

Boards should work with the senior executive team to ensure that roles, responsibilities, delegations and risk appetites in responding to Log4j are clearly defined. Executives such as the CIO or CISO are ideally placed to lead the organisational response. Boards should also consider nominating a Director -- ideally with relevant cyber security, operations or risk management skills -- to interface between the Board and the senior executive team to ensure board level decisions can be made quickly.

The Log4j vulnerability is a critical incident that will likely have a long tail, and may require surge resourcing or establishment of a dedicated tiger team to address appropriately.

What is our plan?

Organisations should develop and enact plans to identify affected products and services. Boards should look to the CIO or CISO to adopt a methodical approach which identifies how the organisation's business is affected or at risk from

Log4j and **provides clear actions to patch or mitigate the vulnerability to reduce exposure and risk**. Large organisations will need a phased approach to manage this issue over many weeks or months, with teams able to sustain a response over the medium term.

If your organisation is a vendor that produces or distributes software, the board needs to know there's a **clear plan to release patches and communicate with customers on impact and mitigations**.

Do we know what hardware and software we have in our organisation?

Your organisation needs to identify what is vulnerable. Boards should be comfortable with the level of continual audit of ICT security and be able to identify impact and severity quickly when new vulnerabilities are discovered. In the Log4j context, IT teams should identify instances of affected software, and whether Log4j has been used in development of internal applications. This task will be easier on corporately-managed assets, but unmanaged and Bring Your Own Device (BYOD) devices may also be at risk. CIOs or CISOs should be thinking about how they will risk manage aging, legacy, or capabilities that have slipped through the net and are not centrally managed (often called 'shadow IT').

Have we patched or mitigated the vulnerability?

Many vendors have reacted to the Log4j vulnerability and released mitigations and patches for the Log4j vulnerability to their customers. Patches for different products are still being released as vendors continue to update their products. Boards should be asking CIOs, CISOs, or response leads whether the organisation has patched all vulnerable systems and if a plan is in place to patch systems and applications when more patches become available over the coming weeks.

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

Boards should engage with the CIO or CISO to **determine what the organisation is doing to detect and prevent attacks, and if sound plans are in place to respond to an incident such as a ransomware compromise.** Organisations should also have plans in place to continuously monitor their systems for signs of compromise, even after

CIOs, CISOs or IT Managers can familiarise themselves with ACSC's Technical Advisory on the Log4j vulnerability which is periodically updated with technical information on how to detect Log4j exploitation and seek incident response assistance.

Boards should also ask whether your organisation is an ACSC Partner. ACSC Partners are able to receive sensitive reporting from the ACSC including indicators of compromise for threat actors. Details are available on cyber.gov.au at https://www.cyber.gov.au/resources-business-and-government/become-acsc-partner.

How will people report issues they find to us?

If your organisation has an internet presence or produces software for customers, organisations need to consider how customers and security researchers are able to report any issues they find. Many cyber security researchers are trying to identify software using Log4j, which may include products your organisation depends on or produces. Organisations should ensure that a technical point of contact is easily reachable by customers and security researchers to enable quick reaction to any vulnerabilities which are identified. If you do not already have one, consider **setting up a help desk for your customers to call or email** to seek advice on how to remediate and mitigate the Log4j vulnerability in your products or services.

As per the Australian Government Information Security Manual, you might also consider **implementing or updating a vulnerability disclosure program**. This will help your organisation engage with security researchers operating in good faith as they identify vulnerabilities in your systems.

Do we know if our supply chain is affected?

If your organisation is dependent on key business partners (such as vendors that supply critical software that runs your business, or a third party with remote admin access to your organisation), you should have an open and honest conversation with them, acknowledging that they will also be trying to understand the severity of the issue. Work together with your vendors and suppliers to mitigate the issues collaboratively.

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

Boards should verify your organisation's end-to-end BCP and crisis response processes against cyber threats to minimise real world impact to the organisation should an attack be successful.

Further information

For more technical information about the Log4Shell vulnerability, the ACSC has released an **advisory** which can be found at https://www.cyber.gov.au/about-us/advisories/2021-007-log4j-vulnerability-advice-and-mitigations. This will be updated as new information is released and as the situation evolves.

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents.

The Essential Eight security controls and Maturity Model is a good baseline to uplift cyber security maturity and make it harder for adversaries to compromise systems. The Essential Eight can be found at https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight.

Information on the ACSC Partnership Program can be found at https://www.cyber.gov.au/resources-business-and-government/become-acsc-partner.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/about-us/about-acsc/contact-us.