CYBILITY

Demystifying Cybersecurity

What you need to know about the Log4shell vulnerability

Orientation for executives, non-executive directors and trustees about 'Log4shell', a new vulnerability that is rated at the maximum 10.

The main facts you need to know:
What is it? Where is it?
Why should we care?
What can we do about it?

WHAT IS LOG4J?

It is an open-source Java logging library that is maintained by the Apache foundation

Its purpose is to log (record) activity in an application

It is used by software developers across the world and can be found buried deep within other applications that may not be obvious on first look

What is the vulnerability?

The vulnerability lies in the way that the application looks up information and ‘translates’ information that is sent to it

By entering a specific combination of characters into a system, attackers can trigger the system to fetch information from an external location on the internet

When the application visits the external location, the attacker tricks the application into accepting malicious code which runs on the server or device and results in a compromise. From here, they can branch out across the organisation's network and compromise other users and systems

Where is it found?

Any application that uses a vulnerable log4j version is affected.
It can be on a server or an end user device

Examples of places that may contain the vulnerability include:

- Any website that has a form to fill in could be vulnerable
- Any web application that we enter data into
- An application installed on someone’s PC
- Someone's internet router at home

Misconceptions

It only affects Apache web servers

Not true – it affects all systems across all platforms that use a vulnerable version of this open source library

None of our internet-facing systems are vulnerable, as their servers are in the demilitarized zone (DMZ)

Not true - exploits show that a string can be entered into one system and as it is passed on to another system on the internal network that uses the vulnerable library – this then initiates the call back to the attacker

We're ok, they won't target us

Not true- because this is so easy to exploit, it was weaponised quickly and attackers are taking a spray approach to identify vulnerable organisations

Why should we care?

This vulnerability scores 10 out of 10 on the scale we use

It is widespread, easy to exploit with little skill, and can be triggered remotely over the internet without logging into the system

So far, the majority of attackers are installing crypto mining software. However, there are cases of ransomware and installations of 'backdoors' so that the attackers can come back later. Some are patching the vulnerability behind them to keep a comprised system to themselves

What can leaders ask their IT and cloud service provider(s)?

1.Are you aware of the Log4J aka Log4shell vulnerability?

If not, why not?

If so:

- What action have you taken to establish if any of the systems in use are affected?
- Have you checked the NCSC-NL list?
- Have you checked if there is any in-house developed or legacy software that may be affected?

2.Are you monitoring for suspicious behaviour and data exfiltration? If so, how?

- Are you searching for internally initiated LDAP connections to external destinations?
- Are you checking DNS logs?

What can leaders ask their IT and cloud service provider(s)?

3.If our systems are affected:

- Which systems are vulnerable?
- What is the potential impact if the data stored within them (or passing through them) were compromised? E.g. data breach of personal data? Loss of IP?
- What mitigation have you taken so far and what actions do you plan to take?
- Have we engaged with our third parties to understand our supply chain risk?
- Have we engaged PR (if you have one) and prepared a statement for our customers (individuals and other organisations) regarding what we are doing to keep their data safe?

Additional Resources

Apache's v2.16 https://logging.apache.org/log4j/2.x/

Apache Foundation https://logging.apache.org/log4j/2.x/security.html

NCSC UK https://www.ncsc.gov.uk/news/apache-log4j-vulnerability

NHS Digital Cyber Alerts https://digital.nhs.uk/cyber-alerts/2021/cc-3989

Curated affected software lists:

MVN Repository

https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-core/usages

NCSC-NL

https://github.com/NCSC-NL/log4shell/tree/main/software

Manual testing (only to be used on sites you/your IT are authorised to test)

https://log4shell.huntress.com

You can also

Listen to this episode:

cybilitysavvy.co.uk

Watch this episode:

cybility.tv

CYBILITY SAVVY

☎ 44 208 040 2846

✉ info@cybilitysavvy.co.uk

🌐 cybilitysavvy.co.uk