Start

Do you have an **inventory** of applications within your organization that use Log4j?

NO →

1. Contact your vendors and request information about the use of log4j in your applications
2. Determine if used software is within the vulnerable software list of the NCSC: https://github.com/NCSC-NL/log4shell
3. Scan your systems using published scan tools: https://github.com/NCSC-NL/log4shell/tree/main/scanning

YES ↓

Do/did these applications use Log4j version **lower** then 2.17.1?

YES → Does your **vendor** have a security update published?

NO → Disable vulnerable classes, wait for **vendor**-updates, consider **disconnecting** internet connected systems

NO ↓ (from lower version)

Monitor future updates on log4j, restart flow in case of **situation-change**

YES ↓ (from vendor update)

Apply **vendor** update (minimal version 2.17.1)

↓

Did you **identify** exploit **attempts** or do you need **help** determining if attacks been performed?

NO → (back to Monitor)

YES → Contact **NFIR**-CERT at 088 133 0700

Implement IDS/IPS monitoring rules / Check for traces of exploitation or **post**-exploitation → (to Did you identify)

IT FORENSICS & INCIDENT RESPONSE

Flowchart version 1.2