Is my organization impacted by log4j?

Detect vulnerable systems

Active Scanning
Source Code Analysis
Vuln & Patch Management

Affected systems found?

YES

YES

Detect & block exploit attempts
Patch systems (Upgrade to v2.16)
Disable Log4j & JNDI lookups

Are vendor-specific patches available?

YES

NO

Use security controls (WAF, IDS/IPS, SIEM, EDR, MDR, XDR, etc.) to detect threats

Implement manual or scripted mitigations

Deploy patches per standard procedures

Compromise detected?

YES

NO

Initiate IR process and procedures
Contact Optiv for additional IR help if needed

Continue looking for threats in case you overlooked something

NO

NO

Affected systems found?

NO

YES