Break the Log4Shell Kill Chain

Security teams are working as fast to patch Log4Shell vulnerabilities as criminals are to exploit them. Here's how these Log4j attacks unfold, and how you can set up lines of defense to protect against them.

INTRUSION

Attackers scan the internet to find vulnerable servers and applications. Then they use an input channel to plant malicious, executable code.

LINE OF DEFENSE 1

Reduce Your Attack Surface

- Identify vulnerable, internet-facing servers to facilitate patching
- Limit internet access to vulnerable machines
- Update web application firewall (WAF) rules to protect against exploit variants

PROPAGATION

The code executes, propagating until it reaches the Log4j library.

LINE OF DEFENSE 2

Stop Lateral Movement

- Isolate vulnerable servers
- Segment your network to enhance protection of your more valuable assets

ATTACK

The victim machine downloads and executes a malicious payload from a command and control (C2) server.

LINE OF DEFENSE 3

Prevent C2 Communication

- Block DNS and domain names used for exploitation
- Map historical communication patterns to facilitate anomaly detection
- Identify and block suspicious outgoing traffic

ATTACK CONTAINED

NORMAL BUSINESS OPERATIONS CONTINUE

Guardicore and Akamai solutions are designed to let you identify and mitigate a wide range of vulnerabilities, including Log4j. Let us know if you have any questions or need help.

Contact us

Akamai

Published 02/22