Recommended Actions

Palo Alto Networks provides protection via Next-Generation Firewalls and Prisma Access. The Threat Prevention security subscription is required. https://docs.paloaltonetworks.com/threat-prevention

With a Threat Prevention subscription you can automatically block sessions related to this vulnerability using Threat IDs. 91991, 91994, 91995 and 92001 (Application and Threat content update 8502). These signatures block the first stage of the attack. SSL decryption needs to be enabled on the firewall to block known attacks over HTTPS. You should verify security profile best practices are applied to the relevant security policies and have critical vulnerabilities set to reset or default actions. https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/threat-prevention/best-practices-for-securing-your-network-from-layer-4-and-layer-7-evasions.html

Additionally, the Log4j RCE requires access to code hosted externally. Palo Alto Networks Advanced URL Filtering security service constantly monitors and blocks new, unknown and known malicious domains (websites) to block those unsafe external connections. Also, suitable egress application filtering can be used to block the second stage of the attack. Use App-ID for ldap and rmi-iiop to block all RMI and LDAP to or from untrusted networks and unexpected sources.

Prisma Cloud can detect continuous integration (CI), container images and host systems which maintain vulnerable instances of log4j. Prisma Cloud Compute Defender agents can detect whether any continuous integration (CI) project, container image, or host system maintains a vulnerable Log4j package or JAR file with a version equal to or older than 2.14.1. In addition, Web Application and API Security (WAAS) rules can be used to detect and block exploit payloads. More information available here. https://www.paloaltonetworks.com/blog/prisma-cloud/log-4-shell-vulnerability/

Endpoint protection is provide by Cortex XDR, using exploit protection on Linux endpoints and Behavioral Threat Protection across Windows, Mac and Linux endpoints. If you are running Cortex XDR Linux agents and content 290-78377 you are protected from a full exploitation chain using the Java Deserialization Exploit protection module. Other Cortex XDR deployments are protected against various observed payloads stemming from CVE-2021-44228 through Behavioral Threat Protection (BTP). Additionally, if you have Cortex XDR Pro and you are using Analytics, you will have post-exploitation activities detected related to this vulnerability.

With a Cortex XSOAR deployment you can also automate incident response. Cortex XSOAR can leverage the "CVE-2021-44228 - Log4j RCE" pack to automatically detect and mitigate the

vulnerability. More information available here.
https://xsoar.pan.dev/marketplace/details/CVE_2021_44228