Log4J Vulnerabilities - Palo Alto Resolutions (Updated to 10 Dec 2021)

The information provided below is referred from https://unit42.paloaltonetworks.com/apache-log4j-vulnerability-cve-2021-44228/ and https://security.paloaltonetworks.com/CVE-2021-44228.

- **CVE Number**

  2021-44228
  2021-45046

- **Discovery Date**

  Dec 10, 2021

- **Threat Level**

  High Impact

- **Response to Log4j**

A remote code execution (RCE) vulnerability in Apache log4j2 was identified being exploited in the wild. Public proof of concept (PoC) code was released and subsequent investigation revealed that exploitation was incredibly easy to perform. By submitting a specially crafted request to a vulnerable system, depending on how the system is configured, an attacker is able to instruct that system to download and subsequently execute a malicious payload.

Due to the discovery of this exploit being so recent, there are still many servers, both on premises and within cloud environments, that have yet to be patched. Like many high severity RCE exploits, thus far, massive scanning activity for CVE-2021-44228 has begun on the internet with the intent of seeking out and exploiting unpatched systems. We highly recommend that organizations upgrade to the latest version (2.16.0) of Apache log4j 2 for all systems. This version also patches the less severe vulnerability CVE-2021-45046, found on Dec. 14.

- **Affected Palo Alto Products**

PAN-OS Panorama 9.0.*, 9.1.*, 10.0.*

- **Palo Alto Protection Products**

Palo Alto Networks provides protection against the exploitation of this vulnerability.

1. **Next-Generation Firewalls or Prisma Access**

   With a Threat Prevention security subscription can automatically block sessions related to this vulnerability using Threat IDs.

   91991, 91994, 91995 and 92001 (Application and Threat content update 8502).

Customers already aligned with our security best practices gain automated protection against these attacks with no manual intervention. These signatures block the first stage of the attack.

2. Palto Alto Recommendation on Firewall

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.

SSL decryption needs to be enabled on the firewall to block known attacks over HTTPS

Customers with log4j in their environments should upgrade or apply workarounds suggested by respective vendors, and not rely only on the Threat Prevention signatures.

3. Cortex XDR

Cortex XDR customers running Linux agents and content 290-78377 are protected from a full exploitation chain using the Java Deserialization Explort protection module Other. Cortex XDR customers are protected against various observed payloads stemming from CVE-2021-44228 through Behavioral Threat Protection (BTP). Additionally, Cortex XDR Pro customers using Analytics will have post-exploitation activities detected related to this vulnerability.

Cortex XSOAR customers can leverage the “CVE-2021-44228 – Log4j RCE” pack to automatically detect and mitigate the vulnerability.

4. 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.