securonix

December 15, 2021

Subject: Securonix Response to CVE-2021-44228: Cloud Customers

Dear Securonix Cloud Customer,

Securonix continues to actively respond to the vulnerability CVE-2021-44228 that was published on December 10, 2021. This is an update to the communications sent on Friday, December 10, 2021.

**Background on CVE-2021-44228 (No Change from Original Communication)**
CVE-2021-44228 is a remote code execution vulnerability in the popular Java logging library log4j2. This CVE was published on December 10, 2021 and can be referenced here: https://nvd.nist.gov/vuln/detail/CVE-2021-44228 with the following detail: CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker controlled LDAP and other JNDI related endpoints. For a description of this vulnerability, see the Fixed in Log4j 2.15.0 section of the Apache Log4j Security Vulnerabilities page.

**SaaS Application:**
**December 10th, 2021 Emergency Maintenance Window**
As noted in prior communications from Friday, Securonix Security, Engineering, and Operations teams spent extensive time analyzing the vulnerability, exploit vectors, and mitigation options across our SaaS solution.

Securonix identified a few vulnerable versions of Log4j in our SaaS offering and took immediate steps to address them. On December 10th, 2021, we **successfully executed an emergency maintenance window and applied the published mitigations across our Application and Cloud infrastructure**. We also updated our Monitoring platform, SnyprEYE, to the current Log4j version.

**RIN Patch to Apache Log4j 2.16:** Securonix is finalizing a patch for deployed RINs updating the version of Log4j to 2.16. We expect this to be available in the next 48 hours and will send a communication once it is available.

**SaaS Application Upgrade to Apache Log4j 2.16**: Securonix is updating our SaaS Application to Apache Log4j v2.16 and will begin coordinated rollouts next week.

**Securonix Threat Labs / Detections Available**
Customers who implemented the new policies and queries that we released in response to this CVE reported that they are successfully alerting on attempts.

Please reference the blog link below for Policies available and associated details:Securonix Apache Log4j Blog and Policies available

securonix

The updated IOCs list can be found here: Log4j IOCs

The Securonix security teams continue to monitor and have not identified any active exploits at this time. Securonix Threat Labs are testing internally and have not successfully exploited this vulnerability.

If you have any questions, please reach out to your Customer Success Manager.

Thank you for being a valued Securonix customer.

Securonix Management Team