securonix

December 15, 2021

Subject: Securonix Response to CVE-2021-44228: On-Prem Customers

Dear Securonix Customer,

Securonix continues to actively respond to the vulnerability CVE-2021-44228 that was published on December 10, 2021. This letter serves as 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 (https://logging.apache.org/log4j/2.x/security.html#:~:text=Fixed%20in%20Log4j%202.15.0) of the Apache Log4j Security Vulnerabilities page.

Securonix Response and Next Steps
December 10th, 2021 Response, Documentation, and Support
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 and took immediate steps to address them in our SaaS Application and document/publish the mitigation steps for On-Prem Customers so Customers/Securonix Support can implement the same.

Starting Friday, Dec. 10, Securonix published the mitigation documentation with ongoing updates and remediation steps for our Application and underlying components as well as Cloudera (via Cloudera documentation). **CVE-2021-44228 Documentation**. Our Support teams continue to be available to walk Customers through these changes. Please open a ticket and put the CVE in the ticket subject to schedule this work.

Next Steps
RIN Patch to Apache Log4j 2.16: Securonix is finalizing a patch for RINs which will update 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.

Release 6.3.1 with Apache Log4j 2.16: Securonix will make available an updated SNYPR 6.3.1 build with Apache Log4j v2.16 available for download/installation. This work is in flight and we will communicate availability later this week.

securonix

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 / https://www.securonix.com/blog/log4j-log4shell-zero-day-vulnerability-cve-2021-44228/

The updated IOCs list can be found here: Log4j IOCs / https://github.com/Securonix/AutonomousThreatSweep/blob/main/Log4Shell/IOCs

The Securonix security teams continue to monitor and have not identified any active exploits at this time.

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

Thank you for being a valued Securonix customer.

Securonix Management Team