securonix

December 10, 2021

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

Dear Securonix Customer

Securonix treats security risks with the utmost criticality and sense of urgency. This update details background, actions taken, mitigation measures, and additional details to help inform you and take the necessary steps to avoid exploitation.

Background on CVE-2021-44228
This is an update to the initial communication sent earlier today regarding the critical vulnerability, CVE-2021-44228, a remote code execution vulnerability in the popular Java logging library log4j2. This CVE was identified 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.

The Securonix Response, Impact, and Mitigation Steps for SNYPR
As noted in the earlier communication today, Securonix Security, Engineering, and Operations teams have spent extensive time analyzing the vulnerability, exploit vectors, and mitigation options across our Application.

We are committed to delivering the highest levels of security and have identified Log4j configuration changes in the SNYPR Application to mitigate risks that are included in this communication. To implement these mitigations, you can work with our Support team or implement yourself. For customers wanting to engage Securonix to make the changes, we have a Log4j Response team to specifically work with you to implement these changes. For any customer that would like Securonix to make the changes, please open a support ticket and add the CVE to the subject - CVE-2021-44228 so that your ticket is routed to our Log4j Response Team who will coordinate making the changes with you. Conversely, your technical resources can implement these changes if they are comfortable doing so. As this is not an Internet facing application, the surface area is reduced when following security best practices.

Securonix Next Steps
Securonix Threat Labs are actively monitoring attacks targeting this vulnerability in the wild using our honeypots and telemetry. We will make our findings available and share with customers.

securonix

For Customers with SnyprEye for monitoring, we are testing / certifying changes and will provide an update within the next 24 hours. We recommend reviewing your security settings for this application for accessibility.

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