WhiteSource

Electronic Healthcare Record (EHR) Software Vendor Remediates Log4j with WhiteSource

CASE STUDY

About

A leading provider of electronic healthcare record (EHR) software has recently been dealing with the newly disclosed Log4j security vulnerability.

The Challenge

On Friday, December 10, 2021, a new open source vulnerability CVE-2021-44228 was disclosed. CVE-2021-44228 impacts the popular Apache Log4j project, and the vulnerable library is found in many code bases across a wide range of applications. By asking Log4j to log a line of malicious code, the program executes that code, which allows malicious actors to gain control over the server in question.

Mitre disclosed this vulnerability with a CVSS of 10. Due to the number of services, sites, and devices exposed, many cybersecurity experts are calling this the worst open source vulnerability of all time.

> We knew immediately that we needed to get ahead of Log4j. Exploits had already been detected in the wild.

The EHR vendor learned about CVE-2021-44228 early in the day. The company knew that it needed to act quickly to secure its many applications or risk exposure. “We knew immediately that we needed to get ahead of Log4j. Exploit attempts had already been detected in the wild,” says their application security architect. Considering that exploit code was being shared publicly, the company wasted no time and began to patch Log4j immediately.

The WhiteSource Solution

Six months earlier, the EHR vendor evaluated several Software Composition Analysis (SCA) solutions, including WhiteSource and Checkmarx. After a POC, the EHR vendor chose WhiteSource to secure its open source software.

Since implementing WhiteSource, the EHR vendor fully scans every code branch in every application. This means that WhiteSource scans more than 2.9 billion lines of code and 4,000 projects each month. In addition, the company uses WhiteSource scan results to identify defects in third-party software then requires third-party software vendors to remediate vulnerabilities based on these scans.

> With WhiteSource, we were able to identify every touchpoint for Java that contained the vulnerability. We have a greater than 98% degree of certainty that we caught every instance of Log4j.

As a result of scanning with WhiteSource, combined with an internal inventory that identified the location of each application on every server across its network, the EHR vendor's application security team had full visibility into its entire code base even before Log4j was disclosed. This made identifying – and eventually remediating – the Log4j vulnerability much easier. "With

The Results

As soon as the Log4j vulnerability was disclosed, the EHR vendor pulled every production repository and started rescanning with WhiteSource. "With WhiteSource, we were able to scan our entire code base to identify and fix every instance of Log4j," says their application security architect.

Because of the granularity of their view into their open source use, identifying impacted Log4j libraries was quick and relatively painless. "For the applications that showed up on WhiteSource with Log4j, we were able to go back to the application owners to ask them to upgrade immediately," says the application security architect. "By midnight on Friday across all of our organization, we were completely patched and pushed to production – all in under 12 hours."