

How a Fortune 100 company solved for Log4j vulnerability — with help from Opsera

Company

Fortune 100
manufacturing

Industry

Diversified technology
and manufacturing

Products Used

Opsera No-Code DevOps
Orchestration Platform

Opsera's no-code DevOps orchestration platform helped the company run code scans, do unit testing, and deploy to development, QA, and production at top speed. Result: The team executed 164 pipelines and 500+ releases in less than 48 hours, fixing their critical Log4j vulnerabilities.

Security is a backbone of software ecosystems. It's more than smart practice — it's also a massive selling point for new customers.

Recently, one of Opsera's clients faced a security crisis when a critical vulnerability was uncovered in the Apache Log4j, a popular Java library for logging in applications. Specifically, it was a new Remote Code Execution (RCE) vulnerability (designated as CVE-2021-44228) in the Log4j. Industry experts quickly uncovered more vulnerabilities, including CVE-2021-45046 and CVE-2021-45105. (A CVE number is the unique number given to each vulnerability discovered across the world.)

Hackers could use these vulnerabilities to get remote access to a company's devices and applications, letting them steal sensitive data or deploy ransomware on servers or devices. Security teams, rightly alarmed, worked full-throttle to identify and patch the Log4j vulnerabilities.

500+

releases (external
& internal apps) in
< 48hrs

3X

improvement in velocity
with built-in quality and
security gates

65%

productivity
improvement with near
real-time insights

The Challenge

Opsera's client is a Fortune 100 company that has been in defense and industry equipment manufacturing for 100+ years. Their IT team helps a wide variety of their technology teams to innovate faster through better intelligence, automization, and other forms of digital transformation across the supply chain.

Before Opsera, even small changes called for time and resources. They had to manually perform unit testing, build the code, run security scans, and deploy to all instances. They knew they needed a better and faster way to automate the end-to-end CI/CD release process across all their technology platforms, speeding results without skimping on security and quality.

The Log4j vulnerability exposed one of any team's biggest obstacles: a lack of visibility and transparency in their libraries. It would normally have taken an IT team more than a week to secure systems against the Log4j vulnerability manually -- obviously not fast enough with the company's security on the line.

The Solution

That's where Opsera's no-code DevOps orchestration platform came into play.

This client was already using Opsera to connect all of its software teams, tools, and information. Opsera's full-featured platform includes no-code CI/CD pipelines with automated quality and security gates and unified real-time insights, plus automated security alerts and granular visibility across their DevOps environments. This sped up the end-to-end deployment of a Log4j fix across hundreds of microservices.

With Opsera, the client's team immediately identified the software components that were compromised. Individual code no longer needed to be scanned manually; in fact, scans can be automated and scheduled to run within Opsera's orchestration platform. This saved the team countless hours and let them turn their focus to building the change to actually fix the issues.

Opsera has integrations with DevSecOps tools like Sonarqube, Twistlock, Anchor, Vault, and Coverity, making everything easier.

Once the team applied the fix for their Log4j version, they used Opsera's no-code pipelines and unified insights to build the code, scan for vulnerabilities, do unit testing, and deploy to all three instances: development, QA, and production. The team executed 164 pipelines and 500+ releases across all environments in less than 48 hours, slamming the door on its Log4j vulnerabilities.

Results and Benefits

Opsera helped the client upgrade its Log4j version with tests, scans, validation, and deployment in less than two days. Better still, the team says it has seen a real transformation in its DevOps processes.

- Real-time visibility into scope of issues (# of apps ethonec.)
- 500+ releases (external & internal apps) in < 48hrs
- 85% faster remediation with Opsera's no-code orchestration platform
- 3X improvement in velocity with built-in quality and security gates
- 65% more productivity with near real-time insights

[Learn More About Opsera and Sign Up For A Demo!](#)

[Schedule A Demo](#)

About Opsera

Opsera's platform allows you the freedom to choose your own DevOps stack - with zero scripting involved. With Opsera, you can automate any stack, build pipelines for any app, and deploy anywhere.

Opsera accelerates best-practice CI/CD adoption so software teams can deliver software faster, safer, and smarter.