MEND | CAE

Case Study - CAE Uses Mend to Secure Applications from the Log4j Threat

About CAE

Based in Montreal, Quebec, Canada, CAE is a high technology company at the leading edge of digital immersion, providing solutions to make the world a safer place. Backed by a record of more than 70 years of industry firsts, CAE continues to reimagine the customer experience and revolutionize training and operational support solutions in civil aviation, defense and security, and healthcare. The company is the partner of choice to customers worldwide who operate in complex, high-stakes and largely regulated environments, where successful outcomes are critical. Testament to CAE customers' ongoing needs for solutions, over 60 percent of CAE's revenue is recurring in nature. CAE has the broadest global presence in its industry, with approximately 11,000 employees, 180 sites, and training locations in over 35 countries.

The Challenge

As CAE's open source use increased, the company became concerned about the security liabilities associated with open source components. An employee from our Global Engineering team had installed Bolt for Azure DevOps, Mend's free tool available on the Visual Studio Marketplace. The Bolt extension impressed the employee enough that he brought it to the attention of our DevSecOps team.

"We initially installed Bolt on one project as a proof of concept," says Hugo Tessier, DevSecOps Specialist at CAE. "Due to that project's success, we quickly saw the added value related to the security that Mend gave us. We then did a full evaluation of Mend and upgraded to their Teams offering. Now Mend is being widely adopted by developers across the company."

When the Log4j vulnerability surfaced, CAE learned about the new vulnerability from a Mend alert. The new vulnerability (CVE-2021-44228), which affects the Apache Log4j project, was released with a CVSS of 10. Given the severity of Log4j, the company knew it needed to patch all instances of the vulnerability immediately.

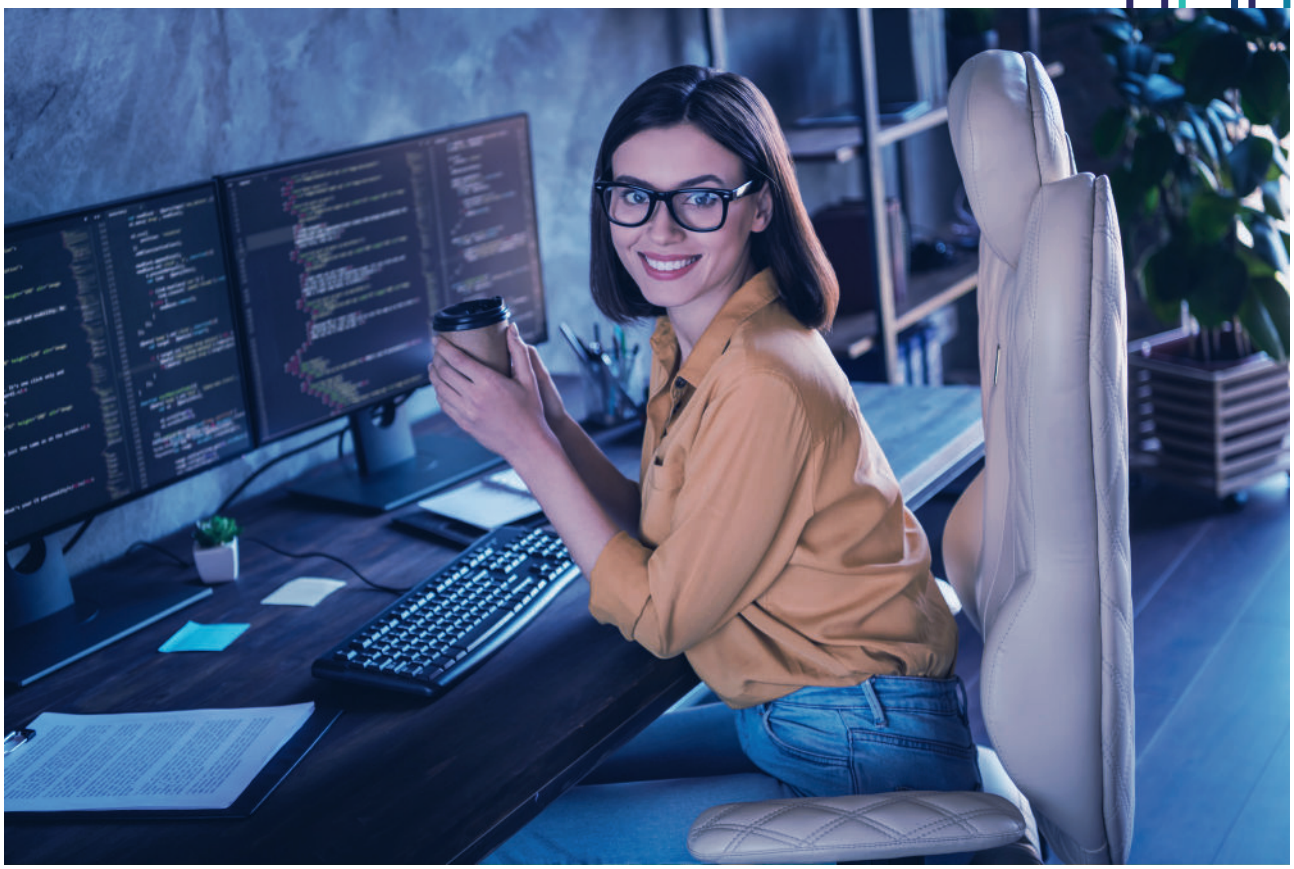
> *Due to that project's success, we quickly saw the added value related to the security that Mend gave us. We then did a full evaluation of Mend and upgraded to their Teams offering. Now Mend is being widely adopted by developers across the company.*

The Mend Solution

CAE scans its projects with Mend in its pipeline as part of the build process. The DevSecOps team uses Mend's scan results to provide feedback with the exact path to any open source vulnerabilities directly to developers so that they can be easily remediated. According to Tessier, "Developers find Mend really easy to use because they get results right in their pipeline, and they can see what is vulnerable and what is not."

When Log4j was announced publicly, the DevSecOps team at CAE knew that it needed to act fast to remediate Log4j throughout all of the company's cloud offerings. Because CAE had been using Mend to regularly scan their open source components, the company's DevSecOps team already had a full inventory of all of its Log4j libraries with Mend's inventory report. "Mend gave us a tangible list of our vulnerabilities," says Tara Vat, Cybersecurity Product Owner at CAE. "That list made identifying Log4j vulnerabilities easy. "

In a very short period of time, CAE was confident that it had identified all instances of the vulnerability. "In less than one hour, we knew we had a complete list of all libraries that contained Log4j," says Tessier. "After that, contacting each project owner to notify them of a mandatory action was easy. Without Mend, it would have taken us at least a week or two just to find all the Log4j libraries."



The Results

CAE was alerted very early on by Mend about the Log4j threat. With Mend in place continuously scanning open source components, CAE was able to identify and remediate the vulnerability across its many projects in very little time. While other organizations were struggling to manage Log4j, CAE had already contacted project owners to implement a fix, significantly reducing its exposure.

Mend was instrumental in CAE's quick Log4j response. "Throughout Log4j, Mend made life easier to report where the problems were instead of going through millions of lines of code," says Vat. "Mend gave us the ability to show our management team actual evidence that our open source components were secure."

> *Generating graphical reports that list our open source inventory and give us full visibility into our open source use is extremely valuable. We have something concrete that we can show to management.*

Reporting isn't the only advantage of using Mend. "In addition to visibility, one of the best benefits of having Mend is that it allows us to inject business rules into the security process," says Tessier. "We can filter results based on severity or reachability to help us prioritize which vulnerabilities to fix first." With Log4j and beyond, CAE is successfully using Mend to reduce its security debt and develop more secure applications.

Related Resources

Learn more at www.mend.io