VERACODE

Beyond Log4j: Improving Open-Source Software Security

Veracode's Chris Wysopal on Understanding and Mitigating Open-Source Risk

ISMG
INFORMATION SECURITY
MEDIA GROUP

VERACODE

CHRIS WYSOPAL

Wysopal is an entrepreneur, computer security expert and co-founder and chief technology officer of Veracode, which pioneered the concept of using automated static binary analysis to discover vulnerabilities in software. He is also a board member of Humanyze and a well-known speaker, author and security expert. Wysopal was instrumental in developing industry guidelines for responsible disclosure of software vulnerabilities. Prior to Veracode, he was vice president of research and development at security consultancy @stake, which was acquired by Symantec. In the '90s, he was one of the first vulnerability researchers as a member of the L0pht Heavy Industries.

Log4j was but the latest fire drill, and it sounds yet another alarm for the unaddressed urgency of open-source software security. **Chris Wysopal**, CTO and co-founder of Veracode, shares insight on how enterprises must define and articulate their own open-source security strategy.

In this video interview with Information Security Media Group, Wysopal discusses:

- The state of open-source software security and how to understand your open-source risk;
- How open-source security can be built into the SDLC;
- Planning now and getting ahead of future open-source vulnerabilities.

STATE OF OPEN-SOURCE SOFTWARE SECURITY

TOM FIELD: What does the Log4j experience tell us about the state of open-source software security?

CHRIS WYSOPAL: A widespread open-source vulnerability like Log4j seems to come along every few years, and you have to just know it's coming and prepare for it. Nothing about the way that open source is developed and

> “There’s more code in your applications that comes from outside the organization than from inside the organization. That’s the norm. You need to have a program for managing the risk that’s coming in from open source.”

consumed has fundamentally changed, so there will be another Log4j-type incident in the future.

OPEN-SOURCE SECURITY STRATEGY

FIELD: Does that mean enterprises should now be defining and articulating their own internal open-source security strategy?

WYSOPAL: Absolutely. Over the last five to 10 years, we’ve slowly used more and more open-source, and 80% of the applications that an enterprise will build will contain different open-source libraries. That means there’s more code in your applications that comes from outside the organization than from inside the organization. That’s the norm. You need to have a program for managing the risk that’s coming in from open source – the stuff that just happens every day and the big ones like Log4j.

UNDERSTANDING OPEN-SOURCE RISK

FIELD: How can you begin to understand your open-source risk?

WYSOPAL: It’s no longer possible for developers to keep track of the open-source they’re using in a spreadsheet because it’s everywhere. So you need an automated solution. If it’s in your pipeline, you can look at the open-source you’re using as you build your software so that you know what goes into production. That’s one way of doing it. Another way is scanning the repos, whether they’re containers or source code repos, where you’re pulling your code from to build. And some people scan in production. You have to do at least one of those things to build up your open-source inventory in an automated way, to know what open source and what version you’re using. With that inventory, you can see what vulnerabilities exist in the software you’re building by looking that up in a vulnerability database like NVD.

OPEN SOURCE IN THE SDLC

FIELD: What are your recommendations for how open source should be built into the software development life cycle?

WYSOPAL: Think before you select an open-source package. Is it maintained by a couple people that don’t maintain anything else and the project is stale, or is it something like the Apache Software Foundation, which has dozens of people working on a particular project? Once you’ve made that

selection, realize that it's going to age over time, like milk. New vulnerabilities will be found, and you'll need to fix them and update your software. Open source is a living thing. It's not "set it and forget it and I'll never have to think about it again." You're going to have to maintain the risk posture of that open source over time.

UPDATING OPEN SOURCE

FIELD: How do you stay up to date on open-source security patching?

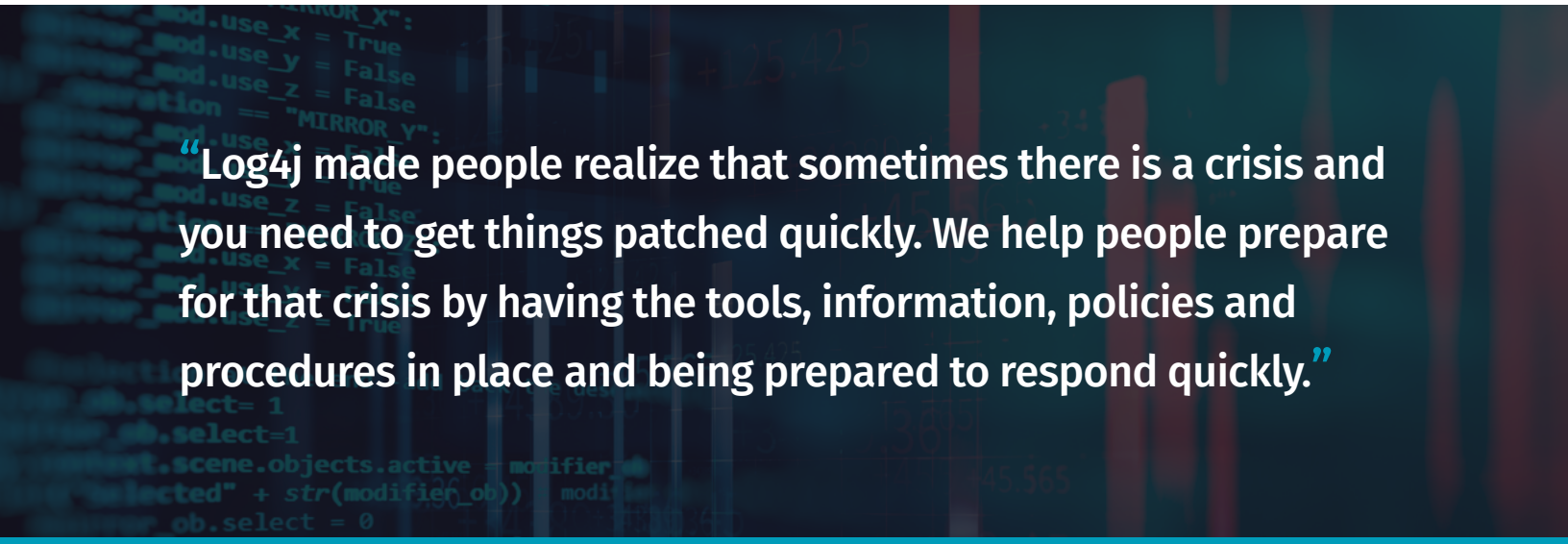
WYSOPAL: You start by having some automation that knows your inventory and can look up what vulnerabilities are there in a vulnerability database. Then you need a policy. When are you going to break the build? When are you going to not push into production? When are you going to drop everything, stop building functionality and patch software? A policy is usually based on the criticality of the vulnerability. For example, it might say: "This is something we can live with for a week," "This is something we can live with for 30 days," or, "This means we have to drop everything." You need a policy that allows you to manage vulnerabilities and still be able to ship your software and the new functionality, which is the reason you're in business.

OPEN SOURCE AND SBOMS

FIELD: Log4j triggered a lot of conversation about the SBOM, the software bill of materials. How does the SBOM movement affect the urgency of open-source security?

WYSOPAL: SBOMs are great because we all consume software that someone else built, whether it's your networking software, your security software or other business applications that some vendor built – Microsoft, Oracle or a small niche vendor that serves your industry and maybe only has 50 developers. The spectrum of software that you consume comes from big companies and small companies, and when a vendor delivers a software bill of materials, which says what open source they're using, that helps you internally track the third-party risk coming from that vendor. It's the only way you're going to know where you'll need to patch.

When Log4j happened, instead of having to call up every single vendor and ask, "Are you affected?



Should I get a new patch of this? Should I be planning for this?" you could just look in your SBOMs and say, "These 15 vendors are going to deliver a fix, and I'm going to have to get my team ready to patch it."

THE VERACODE APPROACH

FIELD: What is Veracode doing to help its customers address each of these fundamentally vital issues?

WYSOPAL: With Log4j, we helped a lot of our customers understand software composition analysis in a crisis environment. That was the use case of that particular situation. It wasn't about opening a ticket for a new vulnerability and saying that you'd eventually get around to patching it. A lot of our customers had dozens and dozens of applications that needed to be updated. Log4j made people realize that sometimes there is a crisis and you need to get things patched quickly. We help people prepare for that crisis by having the tools, information, policies and procedures in place and being prepared to respond quickly. Part of that is education, and part of it is staying up to date.

Some people ran into problems because they were so out of date with their usage of Log4j that it took a big engineering effort to update, which shows that you don't want your open source to get stale. You don't want it to be multiple years old, because sometimes you'll have to do a major revision and it will take many days of development time to update that library. We work with our customers to prepare them so that they can respond quickly. And staying up to date and having the right automation in place makes a huge difference.

VERACODE

Veracode Envisions a World Where Software Is Developed Secure From the Start

You're focused on work that creates the blueprint for the future. Lean into Veracode as your partner for developing secure software to achieve your business objectives, while gaining a competitive edge.

We work with security and development teams to build an advanced application security program – one that reduces risk of security breach and accelerates your business. With a powerful combination of automation, integrations, process, and speed, you get accurate and reliable results to focus your efforts on fixing, not just finding, potential vulnerabilities.

Click here to learn more: **www.veracode.com**

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io