Lowenstein Sandler's Cybersecurity Awareness Series

Session 4-
The Flaw in Log4j and How It Can Impact Your Business

By Kathleen McGee and Ken Fishkin
DECEMBER 2021

Kathleen McGee: Hi and welcome to Lowenstein Sandler's latest in our Cybersecurity Series. I'm Kathleen McGee. I'm a partner in our White Collar and Tech Group practices. And with me today is Ken Fishkin from Lowenstein Sandler. We're here today to talk about the latest, massive vulnerability, truly rocking the global software stage and why the stakes are so high for viewers.

They're high because it's not just a necessary patching event, but because everybody should be considered on notice. And if you're not protecting, you're placing yourself in a other vulnerability from a legal perspective. Ken, can you tell us a little bit more about the specific software vulnerability and how we can start to fix it?

Ken Fishkin: Kathleen, on December 9th vulnerability was released to the public about this huge problem because it affects all applications that have Java in it. And as a result, millions of applications all over the planet are impacted by it. And since it was released to the public and not given to the developers, privately, all these developers now have to scramble and put patches on right away before they get exploited by these actors who could put ransomware on them. This is called the Zero-Day Vulnerability. And this could impact businesses, games that gaming companies for example, like Minecraft or even spacecrafts, all these companies use Java--or throughout the world, your HVAC system, anything that you can think of might be using this application and might need to be patched.

That's why this is such a big problem in our industry and it's so easy to exploit as well. That's what makes it a high severity.

Kathleen McGee: Ken, let me ask you, does this particular vulnerability have a name in case our viewers want to do some independent research on the problem?

Ken Fishkin: Yes, it's called LogShell or a Log4j.

Kathleen McGee: So Ken, now that our viewers know that this software vulnerability is literally everywhere. What can they do to fix it?

Ken Fishkin: So that's really a great question, because think about it like knowing where all the AA batteries are in your house, you don't really know exactly where they are, but you have some kind of idea and that's what developers are doing right now.

They're scrambling, trying to find where this vulnerability is within their applications. And these applications are not just business applications we deal with. They could impact HVAC. They could impact networks. Software is embedded in all of hardware and Java is really a key components in millions of different applications.

And that's why everybody's scrambling, working overtime to get these patches installed.

Kathleen McGee: It's both fascinating and frightening. I think one thing that leaps to mind for a lot of people, when they think about this patching and re-patching effort, is the business cost, the interruption that's likely going to happen with these sorts of necessary stops and starts for patching.

But one thing that comes to mind for me is if you don't patch, you're that much more vulnerable to ransomware. I know that you and I have talked about ransomware in depth in one of our other cybersecurity sessions for Lowenstein Sandler. I've heard you tell me before that there are already ransomware actors on the prowl with respect to this latest event.

Can you tell us more about that?

Ken Fishkin: Yes, so whenever there's a vulnerability that's this severe and this easy to deploy, there's going to be ransomware and other malicious attacks immediately following it. So there's already been spottings of ransomware attacks by these ransomware gangs, these criminal gangs.

And that's really the issue at hand right now. It's less about making sure that the patches are installed, but more about preventing gangs from exploiting ransomware on their systems.

Kathleen McGee: Which would no doubt, completely shut down your business and cost far much more in terms of time and concern for our viewers.

The other thing that has been coming to mind a lot with this most recent vulnerability is the fact that it has been highly publicized. If our viewers hadn't heard about it yet, rest assured it is all over the news and certainly going to be the subject of interest for some time to come. And that means that other lawyers and regulators have an expectation that if you hear about it, you're going to fix it. If you don't fix it, then you will be considered likely liable for any resulting harm that happens. So from the lawyer's perspective, it's really critical that you take all reasonable efforts to patch, scan and re-patch to the extent possible.

Ken Fishkin: Exactly. If you do not do everything possible to patch your systems and show that you are doing everything in your power to protect your systems, then you might be in violation of these regulations.

Kathleen McGee: And subject to really not just business interruption, but civil liability, both from regulators and from the plaintiff's bars.

© 2021 Lowenstein Sandler LLP

The contents of this website contain attorney advertising. Prior results do not guarantee a similar outcome.

One big concern that everyone should have on their mind is if you're not patching, it could be read that you're not protecting. You're not protecting your own business and you're not protecting the privacy and data security of others whose sensitive information you might be protecting. If that's the case, it's quite likely that someone's going to be pursuing you for violating data security or privacy provisions under state or federal law.

So it's really important that you stay vigilant patch and protect, not just for other people, but for your own interests as well. So be vigilant, do your patches and for questions, please, don't hesitate to reach out to your Lowenstein Sandler contact, to Ken or I directly, or to visit our website at lowenstein.com.

Thank you so much for joining us today on our latest in the series on cybersecurity. Ken, thank you as always for being my partner in this.

© 2021 Lowenstein Sandler LLP

The contents of this website contain attorney advertising. Prior results do not guarantee a similar outcome.