Heather:

Welcome to the Hurricane Labs podcast. I'm Heather, and today we're going to be talking about log4j. Yes, yes, log4j again. So last year, President Biden issued his executive order for improving the nation's cyber security. In February this year, the Department of Homeland Security announced the establishment of the Cyber Safety Review Board, or CSRB, and the first order of business for that board was to issue a report including a review and assessment of vulnerabilities associated with log4j, recommendations for addressing any ongoing vulnerabilities and threat activity, and recommendations for improving cybersecurity and incident response practices in policy, based on the lessons learned from the log4j vulnerability.

Heather:

Now that report was released on July 14, so it just became available and joining me today to talk about it, and the board, we have our Director of Security Operations, Josh Silvestro and one of our soft architects, Meredith Kasper. Thanks for joining me. I appreciate you taking the time.

Josh:

Absolutely. Thanks for having me.

Meredith:

Yeah, it's a pleasure to be here.

Heather:

What are your thoughts about Biden's executive order and the CSRB. How do you see them impacting the industry as a whole?

Josh:

I think, personally, from my perspective, I'm very supportive of it. Now we know that there's a dedicated government group that will be overseeing new disclosures, kind of doing deep dives, providing insight and reports around it. And, truthfully, when anything like log4j happens, a good source of information that you know that's going to continue to exist is always great. On top of that, organizations change, companies change, so knowing potentially that this CSRB group could stick around, it's good to know that we're likely to expect a steady stream of content. And, truthfully, at the end of the day, all information's good information. It's quite possible the CSRB will be doing a deep dive, find a bunch of information that's really helpful. However, there's still third party organizations, whether it's someone like us, Hurricane Labs, or other MSSPs out there that are doing security research that are going to find additional information. So I think the more you can get, the better. Just that way, you can paint a really wide and detailed picture to understand threats against your environment.

Heather:

So let's talk about some of the review board's recommendations regarding log4j. What points did you find particularly worth highlighting?

Josh:

Yeah, so I think there's a lot of good points here. And on that same note, I also don't think any of these things are groundbreaking. A lot of these go back to fundamentals of vulnerability management for any business. It is just nice to see stuff coming down from government boards and such to lay them out because while there's a lot of good places to find resources, at least in my experience, a lot of people tend to fall back and trust on CISA and other releases that come from the government because, at the end of the day, they probably have better intelligence to some extent in areas that maybe average businesses aren't aware of. So it's really good information that kind of comes down the pipeline and gives people a good source of truth to trust. I think some things coming out of this that are worth highlighting and talking about are things such as the organization should be prepared to address log4j vulnerabilities for years to come. Part of that is just due to some software that has to be used by businesses that just won't be receiving updates because maybe they're out of date. Maybe some softwares that aren't even aware that they still have log4j vulnerabilities or similarities in the vulnerability that could be exploited in the future. It's worth noting things like this. Some people might say, "Well, if it's patched, why are we going to see it for years?" We still see EternalBlue and SMB exploits from years ago in Windows environments that also have a patch available that either, for aging equipment, they can't replace because it's not available or other business reasons. Still has that vulnerability in their environment and creates issues. I think the other point worth highlighting here is how the report calls out things such as organizations should be investing in capabilities to identify vulnerable systems, whether that is through vulnerability management or even internal policies to help regulate, check and kind of rinse and repeat that process over and over again. So as new vulnerabilities are discovered or things such as log4j continue to stick around or evolve over the years, that organizations have the capabilities to identify those and handle new vulnerabilities in their environment that might pop up, whether they're expected or unexpected.

Heather:

That should include having a vulnerability disclosure plan in place. It's something that we've talked about before. We had a podcast with one of our pentesters, Dennis, where he had really a heck of a time disclosing of vulnerability. You have these pentesters who are trying to do the right thing and trying to share with a company that they found something that makes the company's site vulnerable. And sometimes not only do these companies not have a plan in place so that pen testers can share what they found, but sometimes they even try to pursue them, right, for, I guess damages. Why is it important in your opinion? Why is it in company's best interest to treat responsible disclosures better?

Meredith:

From my perspective, I think it's really important to ensure that you're allowing for the option of responsible disclosure. Because if somebody is acting ethically and their goal is to help you in your best interest to prevent further security flaws, bugs, whatever the situation may be in that specific case, they are essentially acting as a free agent for your company. Using a program such as HackerOne or just even stating a responsible disclosure policy on your website so people know whether or not it is, in fact, safe to engage if you believe you may have found something is critical for helping you decrease your own threat landscape.

Josh:

Yeah, absolutely. And I think even taking that a little bit further. A lot of times you see in the news, or maybe even through Twitter threads, that a lot of organizations take it immediately as, "Hey, why are you doing that thing" Now, I know it's the equivalent of walking by a house late at night and seeing a door wide open to kind of walk up, knock on it and say, "Everything okay in there?" Make sure people are okay or whatever. Some neighbor might say, "Hey, things are good. Thanks for checking." Or maybe, "Something's wrong. Thanks for finding me." However, a lot of organizations typically take it as, "Why are you knocking on my door? Get out of here. It's not your business." And they do. They kind of come back and pursue charges or other legal ramifications for someone disclosing that vulnerability, which all that does is it prevents people from disclosing those things in the future. It's not uncommon to see on Twitter someone say, "Hey, I found this vulnerability. I don't know how to disclose it because I don't want to get arrested, but I'm also not trying to act unethically and I want this company to know. How do I go about it?" Personally, as a consumer of many products and especially in the digital age a lot of digital products, I would rather have someone say, "Hey, we found this thing. Here's what we did to fix it. Here's how it affects you, if at all, and here's what you need to do." That's way better, in my opinion, than some of the organizations who decide not to disclose it or not even engage with the person trying to report it. And then finding out three, six months, or even a year later that this thing happened and they never disclosed it and kind of feeling uneasy about them. I think it just makes sense to, especially the people that approach the disclosure in a ethical and appropriate manner, to kind of embrace that, work with them. Because a lot of times they'll be willing to provide more information. Give them a timeline on what your plans are to address it so that way, they typically will come back and say, "Yeah, that's great. Once you've addressed it, let me know so I can release this publicly." And it's a really good relationship and a lot of the organizations I've seen kind of foster that and embrace it have really flourished on that front, while other organizations who haven't tend to get a lot of pushback from the info sec community as a whole.

Heather:

Shifting back to log4j and talking about community collaboration, let's talk about what they have to say about open source and software development.

Josh:

Open source software's obviously appealing because in a lot of instances it's free or low cost. And due to that, a lot of organizations opt to adopt it. So I think through that, people developing open source software, it's really important that they're taking the time to securely develop the code as well as bring in third parties to do testing on it, code review, make sure that things that are being released are protecting the organizations using it. On top of that, on the topic of vulnerability management disclosure so on and so forth, it's important for open source software developers as well to have vulnerability management plans in place. When a vulnerability is found, how do they quickly address it and release new code to update and patch that vulnerability for their users?

Heather:

How do their recommendations for dealing with log4j relate to cybersecurity as a whole? Are any of these recommendations more generally applicable?

Meredith:

Yeah, the one I would say is the biggest and arguably most important is ensuring that you've got some form of vulnerability management program and identification system. That's really crucial for ensuring that you stay on top of your organization's cybersecurity threats and knowing exactly what is on your network, where that is, what that's tagged as, whether it be a critical system, an end point, even something as simple as a PLC or an ICS device. Knowing exactly what each item is, where it is, what services it's running and then, of course, tying into the vulnerabilities themselves what specific softwares they're running so that when something like log4j does come out, you know this system has this software, this software is vulnerable to log4j, this is something that I need to keep more eyes on. And making sure that you stay on top of that and ensure that with both vulnerably management, asset management and IP address management, that you've got them all functioning together and working together as essentially a cohesive unit. And I go into this a little bit further on my blog on vulnerability management and the importance of making sure that vulnerability management and asset management are working together and you're actually using that in your centralized logging platforms, such as Splunk and ensuring that all of this information feeds together nicely and that you are able to maintain this and keep it up to date consistently.

Heather:

So how can companies be proactive when it comes to managing their vulnerability?

Meredith:

The easiest way is to always be monitoring for vulnerabilities, both by monitoring for known vulnerabilities that are being exploited out in the wild, as well as signatures for vulnerabilities using something like an IDS or even an IPS, if you'd like to proactively block that traffic. And then having a plan to remediate quickly when something is exploited and vulnerable, as well as block any of that traffic as soon as it's seen. Because that will allow your organization for a significantly faster response time and a bit of a proactive approach to a potential attack, whether or not that is, in fact, targeted.

Josh:

Exactly. And the easiest way to start that process is to assign ownership to certain people or a group that are going to oversee the vulnerability management program, get them on a regular schedule of review, whether that's a weekly, biweekly, or monthly basis, where they look at those vulnerability reports they're receiving from whatever internal products. Or once they've established a good asset inventory and they know what's running where, just getting together on a regular cadence to look at new disclosures and see what's applicable to the environment. Or in the case of log4j, if you had all those things in a row and you find out about the log4j vulnerability, you can quickly review your asset inventory to understand what's running where and what critical assets you need to patch or worry about. It saves a lot of headache. It saves a lot of panic when you know where everything is. And we've seen this time and a time again with things like log4j or, again, EternalBlue, some printer exploits we saw last fall. It's not uncommon that those things are kind of out of sight, out of mind. And then as soon as it happens, there's a lot of panic to find out what's running where, how do we identify it. And those are really the worst times to try to do those things. Because on top of the panic about potential exploit, now you're trying to find any rogue systems that you weren't aware of that are running the vulnerable software. So if you wanted to get started, I'd recommend just getting a team together, getting on a regular cadence to review reports as well as look at new disclosures and see how those affect your environment.

Meredith:

And that's a really good point as well. Making sure that you've got some form of rogue device detection on your network is critical just for maintaining knowledge about what assets you have and where. Because those won't traditionally always show up in an asset management program, simply due to the fact that they're a rogue device that you haven't previously tagged and your systems don't know what they are. So making sure that there are no unknown devices on your network at any given time is really important as well.

Josh:

And, lastly, on the topic of vulnerability management, something that some people don't often consider is that you can typically lean on your SIM quite a bit to help identify vulnerabilities. You still need a product such as a Qualys or a Nessus scanner to do vulnerability scanning and management or an IDS on your network to actively detect threats. However, if you put that information back into Splunk, you can do a lot of useful things to help with your review of vulnerabilities, whether that's a dashboard that you can pivot into daily to see any new high or critical vulnerabilities, whether it's in a case like log4j, where you quickly want to understand where those vulnerabilities are in your environment. You can again have a dashboard or run a couple Splunk queries that will help identify those things. Furthermore, it's a good way to help identify potentially rogue systems on your network. Let's say you've patched something like log4j and you don't expect to see it again. You can still have a regularly scheduled report or query that runs looking for log4j related vulnerabilities. Once that pops up, Splunk or your SIEM of choice can then generate an alert back to your team to say, "Hey, host with a log4j vulnerability was found on the network and you should look into that." It's a great way to, as vulnerabilities evolve or maybe kind of fall at a site as new things come up, it's a good way to still be alerted to those vulnerabilities or potential threats in your environment without having to turn a complete blind eye to them.

Meredith:

It's also very useful for your security operations center to have that data in Splunk. That way, if somebody externally is scanning for something like log4j or attempting a log4j exploit, you are easily able to hop into your SIEM and essentially say, "This is the traffic we're seeing against this specific host, per the last Qualys scan that we had." This host is not vulnerable to log4j so this isn't going to be a true positive event and be able to cut down on some of that noise as well.

Heather:

All right. That's all for today. Thanks for joining us and do be sure to check out our resources for the blogs that we mentioned in this podcast. And until next time, stay safe.