Reevaluating Organizations' Cybersecurity Needs After Log4j

By **Colin Jennings, Ericka Johnson and Michael McAndrews** (January 19, 2022)

Colin Jennings

Ericka Johnson

Michael McAndrews

Just in time for the holiday season, and at a time when cybercriminals are generally most active, industry experts discovered a critical vulnerability in a software commonly used by companies.

The software, Apache Log4j, is a popular Java library for logging in applications. The vulnerability enables a remote attacker to take control of a device, potentially enabling cybercriminals the opportunity to steal sensitive data and deploy ransomware.

To combat this potentially devastating operational and legal outcome, information technology security teams have been feverishly implementing patches to fix this vulnerability. Over the holidays, network scanners everywhere have been abuzz, searching for unpatched vulnerable systems.

However, many organizations have found that they lack full inventories of all the software they use, making patching difficult and a never-ending game of whack-a-mole. Further, vendors and cloud-service providers are still struggling to issue fixes to all of their software products.

To add to the feeling of exhaustion and discontent, researchers say this flaw has been around for years, some estimate back as far as 2015. According to U.S. Cybersecurity and Infrastructure Security Agency Director Jen Easterly, the vulnerability is already being used by a "growing set of threat actors."

As such, industry experts expect that this incident will follow a pattern like the Hafnium attacks in March 2021, where the whack-a-mole approach proved far from sufficient.

In the Hafnium attacks, where cybercriminals exploited vulnerabilities in Microsoft Exchange, cybercriminals engaged in large-scale exploits of this zero-day to obtain initial access across a large footprint of organizations. In that case, web shells were deployed and exploited months later, frequently ending in file exfiltration and then ransomware.

As such, while many companies patched their systems, the patching was insufficient because it occurred after the attackers established their persistence.

The key failure in the Hafnium story is that many organizations focused solely on patching their systems and failed to further investigate for signs that the attackers were already present. Such indicators include, for example, Cobalt Strike beacons, strange DNS requests and other possible instances of command and control activity.

Unfortunately, for victims of the Hafnium attacks, the results were costly.

What should my organization consider implementing going forward?

Government cybersecurity agencies in the U.S., Canada, the United Kingdom, Australia and New Zealand — collectively known as the Five Eyes — issued a joint cybersecurity advisory on Dec. 29, 2021, to provide guidance on addressing Log4j vulnerabilities. From a technical perspective, they recommend an organizations plan addresses each of the following technical three elements:[1]

1. Identifying assets affected by Log4Shell and other Log4j-related vulnerabilities;

2. Upgrading Log4j assets and affected products to the latest version as soon as patches are available and remaining alert to vendor software updates; and

3. Initiating hunt and incident response procedures to detect possible Log4Shell exploitation.

From a nontechnical perspective, on Dec. 17, 2021, the U.K.'s National Cyber Security Centre likewise issued guidance for board members of medium to large organizations. In particular, they asked organizational leaders to consider the following questions:[2]

1. What is our plan for responding to this incident? Who is leading on our response? Do they have prerequisite resources and experience to execute the plan?

2. How will we know if we're being attacked, and can we respond? Is there evidence of prior exploitation of this vulnerability?

3. What percentage visibility of our software/servers do we have? Do we have an adequate inventory of assets to allow quicker identification next time?

4. How are we addressing shadow IT and appliances? And any bring your own devices and applications?

5. Do we know if key supply chain providers are covering themselves adequately?

6. Does anyone in our organization develop Java code? If so, how will people report issues they find to us?

7. When did we last check our business continuity plans, disaster recovery and crisis response?

8. How are we preventing technical teams from burning out?

While every entity's cybersecurity needs are different, organizations should ensure that they have implemented at least the following as part of their comprehensive approach to answer these questions and mitigate its risk of a cybersecurity incident.

Conduct a cybersecurity risk assessment.

In general, the purpose of an assessment is to identify cybersecurity vulnerabilities in an organizations policies, procedures, and IT environment and to provide remediation strategies as appropriate.

For the Log4j cybersecurity vulnerability, an assessment may identify exploit attempts and secondary attackers' actions, which include deploying crypto miners, ransomware, botnet activity and commodity malware deployment.

Prepare a written cybersecurity policy.

A written cybersecurity policy sets forth an organization's policies and procedures for the protection of its information systems, particularly its sensitive business information. The cybersecurity policy should address key areas of concern, to the extent applicable, such as data governance and classification, customer data privacy, and vendor and third-party service provider management.

To instill a tone-from-the-top culture, the cybersecurity policy should be approved by a senior officer or the organization's board of directors.

Develop or update your incident response plan.

Many industries and jurisdictions require organizations to have a policy addressing how the company with effectively respond to a cybersecurity incident, like a large-scale exploit of the Log4j cybersecurity vulnerability. An incident response plan sets forth the key steps that organizations need to immediately take during a cyber incident.

For example, an incident response plan will set forth reporting escalation procedures, alternative communication plans and will create a response team of stakeholders and outside experts to assist with the response.

Ensure your personnel are adequately trained.

Organizations should provide regular training for all personnel based upon the risks identified in the assessment. Given that a common method of attack is through email phishing or downloads from malicious websites, an effective defense mechanism is to train your personnel on the basics of cyber hygiene.

Likewise, your response team should conduct at least yearly exercises to practice its response in accordance with the incident response plan. Having a well-trained incident response team in place prior to an attack, positions organizations to efficiently act in a measured, calm and unified manner.

The Log4j vulnerability is a significant event with major ramifications. History shows that inaction now leads to potential compromise later with devastating operational and legal impacts. The time to act is now.

Colin R. Jennings is a partner and Ericka A. Johnson is a senior associate at Squire Patton Boggs LLP.

Michael McAndres is chief technology officer of PacketWatch.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Adapted from: https://www.cisa.gov/uscert/ncas/alerts/aa21-356a.

[2] Adapted from: https://www.ncsc.gov.uk/blog-post/log4j-vulnerability-what-should-boards-be-asking.