

Federal Agencies Sound Alarm on Widespread Log4j Cybersecurity Flaw: How Should Organizations Respond?

Jami Vibbert, et al.



Arnold & Porter

January 11, 2022

Federal Agencies Sound Alarm on Widespread Log4j Cybersecurity Flaw: How Should Organizations Respond?

Advisory

By Kenneth L. Chernof, Ronald D. Lee, Jami Vibbert, Daniel E. Raymond, Jason T. Raylesberg

As a result of the recently discovered vulnerability in the commonly used programming code known as Log4j, almost all organizations in all industry sectors face potentially significant reputational, economic and legal risks. Given the low level of sophistication required to exploit the flaw—one described by Cybersecurity & Infrastructure Security Agency (CISA) director Jen Easterly as “one of the most serious I’ve seen in my entire career, if not the most serious”—a range of malicious actors, from amateur cybercriminals to nation-state cyber-hacking organizations, could use it to wreak damage upon computer systems powering everything from essential utilities to consumer electronics. Indeed, Microsoft reported that the vulnerability was being used by multiple nation-state groups originating from China, Iran, North Korea, and Turkey, and the Belgian Defense Ministry confirmed a December 13 Log4j-related attack prompted it to shut down portions of its computer network.

Hackers generally have exploited the vulnerability for the purpose of crypto-mining, credential theft, and data exfiltration. Although fallout from the vulnerability is in its nascent stages, it is clear that Log4j may very well match if not exceed the level of threat to security in the US and abroad, businesses’ wellbeing, and privacy of consumer data posed by the December 2020 SolarWinds attack. To safeguard company and customer data, reduce the risk of business interruption, and minimize potential liability in connection with future civil suits and/or enforcement actions, organizations should take steps now and over the coming months to actively assess this threat and deploy effective mitigation and prevention measures.

What is Log4j?

Log4j, created by volunteers within the Apache Software Foundation, is a Java-based logging library that can be run across platforms such as Microsoft Windows, Linux, and Apple’s MacOS. These libraries create records of computing activity that are then reviewed by engineers to troubleshoot issues or track data within their programs. By exploiting the Log4j flaw, bad actors can seize control of an affected system and accomplish any number of harmful goals. Log4j’s ubiquity renders the vulnerability especially dangerous, as it is present in web servers ranging from those powering HVAC systems to those used in the operation of the popular sandbox video game Minecraft.

Key Recommendations

Monitor Regulatory Guidance

United States and other government agencies have published guidance that instructs organizations on ways to effectively respond to the Log4j vulnerability. In so doing, regulators have previewed what mitigation and prevention measures they

would likely consider to be reasonable as a baseline when evaluating organizations' conduct in connection with any Log4j-related investigation or other administrative action.

Organizations should pay particularly close attention to CISA's [webpage](#) dedicated to Log4j. Updated regularly, the site describes technical measures organizations should take, including links to the most recent patches for Log4j. It also features a compilation of resources to consult in responding to and remediating any issues, among which is a community-sourced [GitHub repository](#) that lists affected third-party vendors as well as a [joint advisory](#) published on December 22, 2021, by CISA, the FBI, NSA, and cybersecurity authorities in Australia, Canada, New Zealand, and the United Kingdom. The advisory recommends specific mitigation steps for organizations, including remaining alert to vendor software updates and initiating hunt and incident response procedures, and reminds organizations of their obligations to report compromises related to Log4j to the FBI or CISA. And it comes on the heels of an [Emergency Directive](#) issued by CISA which directs US federal civilian executive branch agencies to "immediately mitigate Log4j vulnerabilities in solution stacks that accept data from the internet."

Organizations should also review any publications issued by industry-specific regulators. The Financial Industry Regulatory Authority (FINRA), for example, recently published a [Regulatory Notice](#) alerting firms to the Log4j vulnerability. In addition to prescribing measures for member firms to adopt to address the flaw, the Notice reminds firms of relevant obligations under SEC Regulations, including S-P Rule 30, which requires firms to have written policies and procedures reasonably designed to safeguard customer records and information, and Rule 4370, which applies to denials of service and other interruptions of firms' operations. The Notice underscores FINRA's expectation that firms develop "reasonably designed cybersecurity programs and controls consistent with their risk profile, business model, and scale of operations."

The FTC similarly published a [release](#) urging companies and their vendors to act now to prevent harm from being done to consumers and to avoid FTC legal action. Noting its intention to vigorously pursue companies that fail to take reasonable mitigation steps in light of Log4j, the FTC points out that the "duty to take reasonable steps to mitigate known software vulnerabilities implicates laws including, among others, the Federal Trade Commission Act and the Gramm Leach Bliley Act." With these warnings in mind, organizations should generally consider how existing statutory and regulatory cybersecurity risk mitigation obligations applicable to them (and others in their respective industries) might be implicated by Log4j, and should promptly formulate a plan to address any gaps in compliance accordingly.

Assess Risk and Make Required Public Disclosures

As a vital initial step, organizations should conduct a comprehensive cybersecurity risk assessment of the extent to which Log4j permeates their operations as well as the resulting threat level. CISA's Log4j webpage contains useful recommendations for technical approaches organizations might take in making these determinations, including consulting the aforementioned Github repository and deploying a [scanner](#) to detect the presence of potentially vulnerable files on an organization's system. Organizations should work to quickly identify any attempts hackers have already made to infiltrate their servers and inflict damage by methods such as the installation of ransomware and deployment of crypto-miners.

In performing these assessments, it is critical that organizations evaluate risks present in products offered by third-party providers and their subcontractors. In addition to reviewing the GitHub repository and using the scanner provided by CISA, organizations should monitor for announcements by third-party vendors of vulnerable products, such as those made recently by Cisco, Red Hat and VMWare. They should also consider formally questioning vendors about possible exposure, including what products they use, how they have evaluated risk, and what mitigation and preventative steps they have taken and plan to take. Note, however, that asking these questions of vendors requires review and follow-up as dictated by the response. These considerations should also be top of mind for companies doing diligence in connection with potential acquisitions.

Following these findings, organizations should determine whether any reporting or disclosure obligations might apply. In particular, public companies should evaluate whether a discovered vulnerability amounts to a material cybersecurity risk that must be disclosed in filings with the SEC pursuant to its [Commission Statement and Guidance on Public Company Security](#)

Incidents. Among other factors, the SEC explains that companies must, as part of making this determination, weigh “the potential materiality of any identified risk and, in the case of incidents, the importance of any compromised information and of the impact of the incident on the company’s operations.” Even if the vulnerability itself does not require disclosure, organizations may want to consider whether and how to incorporate this and similar types of vulnerabilities into annual filings.

Conduct Tabletop Exercises and Review Incident Response Plans

Organizations should also ensure they are adequately prepared to respond promptly and appropriately to any incident that might arise from the Log4j vulnerability, both in terms of identification and remediation of an attack, notification to customers, regulators, and other relevant stakeholders, understanding insurance coverage, engaging forensic teams and ransomware negotiators, and collaborating with law enforcement. Tabletop exercises simulating a Log4j-related intrusion could prove particularly helpful for organizations seeking to refine their incident response procedures and playbooks. In line with the FTC’s [general guidance](#) that “a strong data security program ensures that a company is undertaking reasonable precautions to protect its network and consumers’ personal information from intruders”, organizations should act with the understanding that regulators might one day scrutinize the steps they took at this time to prepare against a possible attack, and document such steps accordingly. Finally, organizations should include, as part of these exercises testing ability to respond to such attacks, discussions on how to handle ransomware payments—whether and how to, what the considerations are, and what the legal risks and considerations are.¹

Conclusion

Actions taken in the coming days and months could make a significant difference not only in the extent to which customer and company data is protected from harm, but also in terms of shielding organizations from possible business interruption and legal liability. It is with this sense of urgency that organizations should develop clear plans to address this flaw in a way that comprehensively addresses all potential attack vectors and attack surfaces.

© Arnold & Porter Kaye Scholer LLP 2022 All Rights Reserved. This Advisory is intended to be a general summary of the law and does not constitute legal advice. You should consult with counsel to determine applicable legal requirements in a specific fact situation.

¹ See our article on how to handle ransomware attacks: *Ransomware is Everywhere: What to Do If You Are Hit* (Jan. 2022).