ALSTON & BIRD

WWW.ALSTON.COM

Privacy, Cyber & Data Strategy ADVISORY ■

JANUARY 13, 2022

The Log4j Vulnerability: What This Critical Vulnerability Means for Your Enterprise

by *Kim Peretti* and *Jon R. Knight*

Over the past month, the public and private sectors have watched with growing concern as the scope of the Log4j vulnerability has materialized. The best up-to-date intelligence on the vulnerability and recommended mitigation steps is originating from security firms and the government through the Cybersecurity and Infrastructure Security Agency (CISA). While the vulnerability itself poses significant potential risks to businesses and their products, there is now also the possibility of Federal Trade Commission (FTC) enforcement or other regulatory review of companies that do not take "reasonable steps" to address the vulnerability.

What Is the Log4j Vulnerability?

Private and public sector partners report that the Log4j vulnerability is the most (or one of the most) prolific vulnerabilities ever reported. The vulnerability is in a Java-based tool from Apache's open-source library used for parsing logs. The tool basically provides a logging system for applications to keep a running list of activities they have performed.

The vulnerability was initially believed to impact Log4j versions 2.0 to 2.14.1 as a way an attacker could engage in remote code execution (RCE). The RCE could allow the attacker to take full control over the system and then steal information, launch ransomware, or conduct other malicious activity. Now, it is also known that vulnerability may also allow for denial of service attacks and may have varying degrees of impact to versions 2.0 to 2.16.

The vulnerability is prolific because Log4j is widely used by enterprise and cloud applications and devices and the affected versions of the applications were released beginning in 2013. CISA has compiled a Github repository identifying potentially affected vendors and software and lists their status (affected, not affected, under investigation, or fixed) and whether or not a patch has been released. This list currently includes thousands of vendors and software products, and government sources indicate that the number of entities ultimately touching resources including Log4j may be in the hundreds of millions.

How Is Log4j Being Exploited?

While the vulnerability was publicly announced on December 9, 2021, the vulnerability appears to have been presented at a Black Hat conference in 2016. While the initial reports of exploitation related primarily to script kiddies finding the vulnerability and dropping bitcoin mining code on Minecraft servers, there are now also reports of follow-on activity including both nefarious criminal activity and state-sponsored actors. Security firms have reported that many existing attackers have added Log4j-related exploits to their existing malware tools and tactics and that exploitation attempts remained high through the end of 2021.

What Is the Legal or Regulatory Risk?

Any significant vulnerability, particularly one that can be exploited to deploy ransomware or potentially provide a foothold for data exfiltration, may pose potential legal and regulatory risks. But now the FTC has warned companies that it "intends to use its full legal authority" against any company that fails to take "reasonable steps" to protect consumers from the Log4j vulnerability. In a January 4, 2022 release, the FTC cautions that the Log4j vulnerability is being widely exploited by a growing number of attackers and poses a "severe risk" to millions of consumer products. The FTC urges companies to "act now" to mitigate threats from the Log4j vulnerability or "similar known vulnerabilities" or risk legal action. Unfortunately, the FTC provides no guidance on what these "similar known vulnerabilities" may be:

> 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. It is critical that companies and their vendors relying on Log4j act now, in order to reduce the likelihood of harm to consumers, and to avoid FTC legal action.

According to the FTC, companies using Log4j should update software packages to the most current version, take steps to identify and remediate this vulnerability, and distribute information about the vulnerability to relevant third parties with consumers who may be vulnerable. The FTC also encourages companies to consult CISA's guidance for additional mitigation steps. However, the FTC's statement does not address the fact that many companies will not be able to update or patch their products until a vendor releases updates or provides further direction, and as illustrated by the CISA Github repository, the list of products pending patches is significant.

How Can My Organization Mitigate This Vulnerability and Associated Risk?

There is no one-size-fits-all approach to the reasonable steps an organization should take to investigate and mitigate the Log4j vulnerability. However, there are general principles and resources that can guide your analysis.

- **Understand your risk posture.** Due to the widespread use of Log4j in both front- and backend systems and applications, it may be very difficult to identify and mitigate all the applications, servers, operational technology, and other systems using Log4j. Moreover, a company may be reliant on vendors to provide patching services when the Log4j vulnerability is built into one of their products. Nonetheless, companies should take steps to understand their possible risk exposure from this vulnerability, including by identifying where an organization is using Log4j as best as possible and the type of data that might be impacted should the vulnerability be exploited. To aid in this identification process, CISA has published lists of resources that can be used to identify uses of Log4j in a company's environment.

- **Once you identify Log4j use, consider published guidance on the mitigation steps appropriate to your organization.** Once Log4j is identified, both private and public sector partners recommend patching if you can (multiple updates from Apache are already available), monitoring if you are able, and segmenting any products you cannot patch so there is no outbound internet access. In addition, these sources also recommend using a web application firewall to block traffic if you cannot patch and cannot segment. More details on CISA's guidance and more-detailed technical mitigation recommendations are available here.

Ultimately, it may take months or even years to know – and mitigate – the full scope of this vulnerability. In reality, how each organization is going to be able to mitigate this vulnerability will need to be tailored to its operations because some may have lesser control or visibility over the systems that run Log4j.

You can subscribe to future ***Privacy, Cyber & Data Strategy*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or a member of our **Privacy, Cyber & Data Strategy Team**:

Kimberly Kiefer Peretti
202.239.3720
kimberly.peretti@alston.com

Kellen Dwyer
202.239.3240
212.905.9340
kellen.dwyer@alston.com

Katherine Doty Hanniford
202.239.3725
kate.hanniford@alston.com

Amy Mushahwar
202.239.3791
amy.mushahwar@alston.com

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333