PRIVATE DIRECTORS ASSOCIATION®
CYBERSECURITY

PRIVATE DIRECTORS ASSOCIATION®
Creating Value Through Board Excellence

December 14, 2021

PDA Cybersecurity Newsflash

Combatting the Apache Log4J Vulnerability

Executive Summary

There has been a significant security vulnerability disclosed by the Apache Software Foundation, a nonprofit that distributes free, open-sourced software. Apache has stated that this software has been "downloaded millions of times," and is widely used by corporate networks across the globe. The ubiquity of this software could impact businesses for months.

This vulnerability notification was released disclosed on Friday, December 10th and has been categorized by US government cybersecurity experts as one of the most significant cybersecurity threats in decades. Additional vulnerabilities were discovered on Tuesday, December 14th.

This briefing is intended to educate you on what is known at this time and prepare you for any incident response or cybersecurity governance discussions on the topic in your board meetings.

What is Apache Log4j Software and how does it impact my company?

Apache's Log4j software is designed to record (or "log") a website's user activities so that security or software development teams can review activities. The vulnerability may allow a hacker to imbed commands in corporate networks in order to steal sensitive data.

Apache's software patch published on December 13th was deemed inadequate by cybersecurity experts as it did not prevent ransomware attacks, "backdoors" that allow hackers to steal sensitive data, or create overwhelming traffic at a company's servers (also known as a Distributed Denial of Service or DDOS attack).

Experts say that ransomware attacks will spike in the near future. Boards need to be prepared.

For Board Consideration

- Ask for management's approach and capability to respond to this cybersecurity threat.
- Ask if all systems have installed the most recent patch and will continue to install patches as soon as possible
- Incident response is a best practice for Boards of Directors, and ensure you are prepared for a ransomware attack.

- Regardless of whether your company has been impacted by this event, Boards should consider instigating an incident exercise to test the company's and board's capabilities.
- Cyber criminals generally seek to steal the crown jewels of the company. Understanding the protection measures of the crown jewels is always prudent. Consider using professional "white hat" hackers to test the network environment frequently and report the findings directly to the Board.
- Boards should evaluate their current cyber risk and risk tolerance expectations.
- The Board should compare their expectations to the risk tolerance plan and investment that management has made in defending and detecting similar sophisticated attacks.
- Third-party vendor risk is significant. Companies must immediately assess the risk from any outside party that has access to or communicates with your company's networks.
- Boards should consider independent, external cybersecurity subject matter expertise in addition to internal for a balanced perspective given recent trends in Board liability.

Fundamentals of the Attack

Cybersecurity and IT experts around the world are actively engaged assessing their environments through security vulnerability scans to determine if they have a version of this vulnerable Apache software. This software is commonly referred to as a "web server" which typically stores and delivers content for a website to the person surfing to that site.

This vulnerability allows the attacker to access the server without the need for credentials (User ID and password). Once inside, the attacker can use this server as an attack point to the organization. The determining factor in the attacker tactics is based on the robustness of the security capability of the organization.

This alert is particularly concerning because this is a ubiquitously used technology that dates back to the mid-1990's and is well-known for being a low priority patch update in IT organizations. Some of the largest technology companies in the world have been hit with issues including attacks against banks, technology firms and general businesses. Initial attacks have centered around organized crime groups seeking to steal money to purchase online, virtual currency like "Bitcoin" or attack the "Virtual Wallets" themselves that users maintain on their computers.

Key Considerations

- Business impact should be considered as a ripple effect. Additional attacks may likely emerge until these vulnerable systems are patched, decommissioned or protected.
- IT teams need to determine the full extent of what occurred to date and stay vigilant for updates as they are released. There are known fixes and protection approaches to defending this attack. Step one is to identify anywhere in the organization where the Apache software may exist.
- Organizations should ensure non-traditional information technologies are assessed as well. This should include IoT or industrial control systems such as security cameras, building control

automation systems, or other systems that may have Apache technology embedded within them, even if not in direct use.

- The attack was preventable with good security fundamental processes and tools. Organizations should ensure they have the advanced detection tools/capabilities to detect the action of hackers once they are inside. Firewalls and Anti-virus programs are not enough.
- Given the head-start the attackers have had and the depth of their potential penetration, affected organizations should not treat this as business as usual. This attack is classified as a Zero Day attack because the companies did not detect that a hack had occurred until their systems were compromised. Leadership should establish an effort with sufficient cybersecurity expertise to ensure network and business system integrity.

PDA's Cybersecurity Committee can assist with providing subject matter expert briefings for Boards who have PDA Corporate Membership. Contact PDA at admin@privatedirectorsassociation.org.

Private Directors Association® Cybersecurity Committee

The purpose of the Private Directors Association® Cybersecurity Committee is to establish PDA as a leading board-level educational and training resource for Cybersecurity oversight best practices in privately-held companies. Our goal is to meaningfully enhance the value that private company Directors bring to their role on private company boards as it relates to Cybersecurity and Privacy issues. As part of that effort, we envision greater private company board representation of independent board members with (documented) Cybersecurity expertise.

Private Directors Association® Mission

Our mission is creating, sustaining and enhancing Private Company value through the active use of diverse Boards of Directors and Advisory Boards. We advocate for excellent practices in board formation and governance. We provide a national network where executives and professionals interested in board service can find and meet with those interested in securing exceptional board members. We provide a welcoming and responsive culture that distinguishes us.

Disclaimer

The Private Directors Association® provides this information as a value to its members and it should be considered general information and not professional or legal advice. The reader should not rely on any information in this document in making business decisions and should seek professional advice. Laws and rules can vary by jurisdiction and members should consult with experts in evaluating their unique situation.