Regulatory Notice 21-42

FINRA Alerts Firms to "Log4Shell" Vulnerability in Apache Log4j Software

December 14, 2021

Notice Type
- Special Alert

Suggested Routing
- Legal
- Legal and Compliance
- Risk Management
- Senior Management

Key Topics
- Cybersecurity

Summary

FINRA is alerting firms to a recently identified vulnerability in Apache Log4J software, which is an open-source, Java-based logging utility widely used by enterprise applications and cloud services. The "Log4Shell" vulnerability presents risk for member firms because they may be using this software in internal applications, or the software may be embedded in third-party software packages. In addition, many applications written in Java are potentially vulnerable.

Bad actors may take advantage of this vulnerability to compromise systems to potentially steal information or engage in fraudulent activities. For example, a remote attacker can exploit this vulnerability to take control of an affected system.

FINRA reminds firms that the U.S. Securities and Exchange Commission's (SEC) Regulation S-P Rule 30 requires firms to have written policies and procedures that are reasonably designed to safeguard customer records and information and FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) also applies to denials of service and other interruptions to members' operations. In addition to firms' compliance with SEC regulations, FINRA expects firms to develop reasonably designed cybersecurity programs and controls that are consistent with their risk profile, business model and scale of operations.

For more information, firms should review the resources provided on FINRA's Cybersecurity Topic Page.

Next Steps

FINRA recommends member firms consider engaging their Technology staff along with third-party vendors, including any IT service providers, and taking the following steps:

1. Leverage indicators of compromise (IOCs) associated with the vulnerability and take the following steps:
    a. Monitor network and server activity to identify attempts to exploit the vulnerability including industry provided IOCs.

b. Review historical log data including past network and server activity to identify IOCs that would indicate a bad actor has exploited the vulnerability in your environment.

c. If the IOCs are confirmed in your environment, consider implementing your incident response plan and handling this as a high-risk cybersecurity incident.

d. If applicable, respond and recover from the intrusion following the steps in your incident response plan.

2. Consider evaluating firm (and, if applicable, vendors') firewalls to address additional risks relating to the vulnerability:

   a. Evaluate firewall rules for outbound traffic and consider adding rule(s) to block traffic to suspicious or unknown locations (*e.g.,* outbound egress filtering).

   b. Confirm that any internet-facing application systems using Apache Log4J are protected by a web application firewall to provide protection against traffic that includes signatures known to be malicious.

3. Review firms' internally maintained application systems to determine if any are at risk from the vulnerability:

   a. Conduct an inventory of all internal systems to identify any that are using the Apache Log4J vulnerable code.

   b. For the systems identified, either apply the security patch for Apache Log4J or upgrade to the latest version of the software that includes the fix (Apache Log4J 2.15 or later).

   c. Test the updated software before releasing into your production environment.

   d. Confirm that the updated Apache Log4j software is applied to all devices that use the software.

4. Evaluate third-party vendors' systems to determine whether they have been impacted by the vulnerability:

   a. Contact your software application vendors and ask them if any of their systems contain the vulnerable Apache Log4j software. For example, vendors such as, Cisco, VMware, and Red Hat have issued advisories about potentially vulnerable products.

   b. If so, ask vendors how they plan to update their system to address the vulnerability.

   c. Receive and test the updated software from vendors before releasing into your production environment.

   d. Confirm that the updated Apache Log4j software is applied to all devices that use the software.

5. Continue monitoring threat information and updates through multiple intelligence sources including, but not limited to:
   a. Cybersecurity and Infrastructure Security Agency (CISA);
   b. FS-ISAC; and
   c. Your preferred threat intelligence sources, including any third-party security systems or tools providers.

Questions regarding this *Notice* should be directed to:

- Dave Kelley, Director, Member Supervision Specialist Programs, at (816) 802-4729 or by email; or
- Greg Markovich, Senior Principal Risk Specialist, Member Supervision Specialist Programs, at (312) 899-4604 or by email.

Additional Resources

- CISA, Statement from CISA Director Easterly on "Log4J" Vulnerability (Dec. 11, 2021).
- CISA, Apache Log4j Vulnerability Guidance.
- Apache Releases Log4j Version 2.15.0 to Address Critical RCE Vulnerability Under Exploitation (Dec. 10, 2021).