U.S. COMMODITY FUTURES TRADING COMMISSION
Three Lafayette Centre
1155 21st Street, NW, Washington, DC 20581
Telephone: (202) 418-5000

Market Participants
Division

Amanda L. Olear
Acting Director

December 14, 2021

Greetings-

The Department of Homeland Security's CyberSecurity and Infrastructure Security Agency ("CISA") has issued guidance concerning a new and potentially serious cybersecurity vulnerability regarding Apache's Log4j software logging application. Although Apache has publicized information about this vulnerability, we are forwarding you CISA's guidance given its potential impact.

Best regards,

Acting Director
Market Participants Division
Commodity Futures Trading Commission

Apache Log4j Vulnerability Guidance

Note: CISA will continue to update this webpage as we have further guidance to impart and additional vendor information to provide:
https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

Summary

CISA and its partners, through the Joint Cyber Defense Collaborative, are responding to active, widespread exploitation of a critical remote code execution (RCE) vulnerability (CVE-2021-44228) in Apache's Log4j software library, versions 2.0-beta9 to 2.14.1, known as "Log4Shell" and "Logjam." Log4j is very broadly used in a variety of consumer and enterprise services, websites, and applications—as well as in operational technology products—to log security and performance information. An unauthenticated remote actor could exploit this vulnerability to take control of an affected system.

Apache released Log4j version 2.15.0 in a security update to address this vulnerability. However, in order for the vulnerability to be remediated in products and services that use affected versions of Log4j, the maintainers of those products and services must implement this security update. Users of such products and services

should refer to the vendors of these products/services for security updates. Given the severity of the vulnerability and the likelihood of an increase in exploitation by sophisticated cyber threat actors, CISA urges vendors and users to take the following actions.

Vendors

- Immediately identify, mitigate, and patch affected products using Log4j.
- Inform your end users of products that contain this vulnerability and strongly urge them to prioritize software updates.

Affected Organizations

- In addition to the immediate actions—to (1) enumerate external-facing devices that have Log4j, (2) ensure your SOC actions alerts on these devices, and (3) install a WAF with rules that automatically update—as noted in the box above, review CISA's upcoming GitHub repository for a list of affected vendor information and apply software updates as soon as they are available. See Actions for Organizations Running Products with Log4j below for additional guidance. Note: CISA has added CVE-2021-44228 to the Known Exploited Vulnerabilities Catalog, which was created according to Binding Operational Directive (BOD) 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities. In accordance with BOD 22-01, federal civilian executive branch agencies must mitigate CVE-2021-44228 by December 24, 2021.

Technical Details

This RCE vulnerability—affecting Apache's Log4j library, versions 2.0-beta9 to 2.14.1—exists in the action the Java Naming and Directory Interface (JNDI) takes to resolve variables. According to the CVE-2021-44228 listing, affected versions of Log4j contain JNDI features—such as message lookup substitution—that "do not protect against adversary-controlled LDAP [Lightweight Directory Access Protocol] and other JNDI related endpoints."

An adversary can exploit this vulnerability by submitting a specially crafted request to a vulnerable system that causes that system to execute arbitrary code. The request allows the adversary to take full control over the system. The adversary can then steal information, launch ransomware, or conduct other malicious activity.

Actions for Organizations Running Products with Log4j

CISA recommends affected entities:

- Review Apache's Log4j Security Vulnerabilities page for additional

information.

- Apply available patches immediately. See CISA's upcoming GitHub repository for known affected products and patch information.
    - Prioritize patching, starting with mission critical systems, internet-facing systems, and networked servers. Then prioritize patching other affected information technology and operational technology assets.
    - Until patches are applied, set log4j2.formatMsgNoLookups to true by adding -Dlog4j2.formatMsgNoLookups=True to the Java Virtual Machine command for starting your application. Note: this may impact the behavior of a system's logging if it relies on Lookups for message formatting. Additionally, this mitigation will only work for versions 2.10 and above.
    - As stated above, BOD 22-01 directs federal civilian agencies to mitigate CVE-2021-44228 by December 24, 2021, as part of the Known Exploited Vulnerabilities Catalog.
- Conduct a security review to determine if there is a security concern or compromise. The log files for any services using affected Log4j versions will contain user-controlled strings.
- Consider reporting compromises immediately to CISA and the FBI.

Resources

This information is provided "as-is" for informational purposes only. CISA does not endorse any company, product, or service referenced below.

Ongoing List of Impacted Products and Devices

CISA will maintain a community-sourced GitHub repository that provides a list of publicly available information and vendor-supplied advisories regarding the Log4j vulnerability.

Ongoing Sources for Detection Rules

CISA will update sources for detection rules as we obtain them.

For detection rules, see Florian Roth's GitHub page, log4j RCE Exploitation Detection. Note: due to the urgency to share this information, CISA has not yet validated this content.

For a list of hashes to help determine if a Java application is running a vulnerable version of Log4j, see Rob Fuller's GitHub page, CVE-2021-44228-Log4Shell-Hashes. Note: due to the urgency to share this information, CISA has not yet

validated this content.

Mitigation Guidance from JCDC Partners

- Microsoft blog: Guidance for Preventing, Detecting, and Hunting for CVE-2021-44228 Log4j 2 Exploitation
- Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Threat Advisory: Critical Apache Log4j vulnerability being exploited in the wild
- Palo Alto Networks blog: Apache log4j Vulnerability CVE-2021-4428: Analysis and Mitigations
- CrowdStrike blog: Log4j2 Vulnerability Analysis and Mitigation Recommendations
- IBM Security Intelligence blog: How Log4j Vulnerability Could Impact You
- Tenable blog: CVE-2021-44228: Proof-of-Concept for Critical Apache Log4j Remote Code Execution Vulnerability Available (Log4Shell)
- Broadcom's Symantec Enterprise blog: Apache Log4j Zero-Day Being Exploited in the Wild content
- Splunk's blog: Log4Shell - Detecting Log4j Vulnerability (CVE-2021-44228) Continued
- VMware Blog: Log4j Vulnerability Security Advisory: What You Need to Know
- Investigating CVE-2021-44228 Log4Shell Vulnerability: VMWare Threat Research

General Cybersecurity Resources

- Joint Cybersecurity Advisory – Technical Approaches to Uncovering and Remediating Malicious Activity provides general incident response guidance.
- NIST Special Publication 800-40 Revision 3, Guide to Enterprise Patch Management Technologies offers more information on the basics of enterprise patch management technologies.
- CISA's Cyber Essentials serve as a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.
- CISA offers a range of no-cost cyber hygiene services—including vulnerability scanning and ransomware readiness assessments—to help

critical infrastructure organizations assess, identify, and reduce their exposure to cyber threats.

- New Zealand Computer Emergency Response Team's Advisory: Log4j RCE 0-Day Actively Exploited