HC3: Alert

December 21, 2021 TLP: White Report: 202112211400

CISA Log4j Scanner Available to Help Identify Vulnerable Web Services

Executive Summary

On December 21, 2021, the Cybersecurity and Infrastructure Security Agency's (CISA's) Rapid Action Force (RAF) made available an open sourced log4j-scanner derived from scanners created by other members of the open-source community. This tool is intended to help organizations identify potentially vulnerable web services affected by the log4j vulnerabilities. The GitHub below repository provides a scanning solution for the log4j Remote Code Execution vulnerabilities (CVE-2021-44228 & CVE-2021-45046). The information and code in this repository is provided "as is" and was assembled with the help of the open-source community and updated by CISA through collaboration with the broader cybersecurity community.

Report

CISA Log4j Scanner on GitHub
https://github.com/cisagov/log4j-scanner

Impact to HPH Sector

Microsoft has observed the CVE-2021-44228 vulnerability being actively exploited by multiple nation-state backed groups originating from China, Iran, North Korea, and Turkey. Furthermore, cybercriminal actors including initial access brokers (IABs) have begun using this vulnerability to gain initial access to target networks. Healthcare and Public Health (HPH) sector organizations are encouraged to take immediate actions to protect against Log4J exploitation. These actions include:

- Discover all internet-facing assets that allow data inputs and use Log4j Java library anywhere in the stack.
- Discover all assets that use the Log4j library.
- Update or isolate affected assets. Assume compromise, identify common post-exploit sources and activity, and hunt for signs of malicious activity.
- Monitor for odd traffic patterns (e.g., JNDI LDAP/RMI outbound traffic, DMZ systems initiating outbound connections).

References

Apache Log4j Vulnerability Guidance
https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
Guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation
https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback