The Federal Communications Commission's Public Safety and Homeland Security Bureau & Office of Communications Business Opportunities Advises the Small Business Community to Take Protective Internet Security Measures Against the "Apache Log4j Vulnerability"

Security officials working for federal government agencies, including the Federal Communications Commission (FCC), recently learned of a serious flaw in a widely used open-source, Java-based logging utility called "Log4j". Agencies are quickly working to mitigate this vulnerability which leaves hundreds of millions of devices open to remote code execution and at risk from hackers and criminal ransomware groups. The FCC urges the small business community to secure its computer networks from the Log4j software vulnerability.

What is Log4j?

Software developers use the Log4j framework to record user activity and the behavior of applications for subsequent review. The nonprofit Apache Software Foundation distributes the Log4j software for free. Log4j is among the most widely used tools to collect information across corporate computer networks, websites, and applications.

Please refer to the federal government agency, Cybersecurity and Infrastructure Security Agency's (CISA), guidance for more information and to stay abreast of developing solutions:

- https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- https://www.msspalert.com/cybersecurity-news/log4j-zero-day-vulnerability-cisa-mitigation-patch-guidance/

If you have questions or want more guidance, please call CISA at (888)282-0870 or the Multi-State Information Sharing and Analysis Center (MS-ISAC), 24x7 Security Operations Center, SOC@cisecurity.org, 1-866-787-4722.

CISA, via the Multi-State Information Sharing and Analysis Center (MS-ISAC), issued the below guidance on the Log4J vulnerability. Per the instructions, recommended mitigation Tactics, Techniques, and Procedures (TTP) are as follows:

CISA RECOMMENDED ACTION STEPS:

December 16, 2021, Updated Steps to Take Now:

1. Run a scan of all software & systems to see if the log4j .jar file is present—go back to November 30 & use this vulnerable hash list.
2. Use the Huntress checker on each system to see if the log4j functionality is present outside of an easily-found .jar file.
3. Look for unauthorized configuration changes on all systems.
4. Block outbound connections at the firewall for any impacted server.
5. Find public statements for each vendor within your network & add them to a tracker to manage over the next few weeks.

6. If the vendor does not have a public statement and they are critical to you, push them for one.

December 14 - UPDATED RECOMMENDATIONS:

- ***The previous patch iteration 2.15.0 does not fully remediate the vulnerability, and thus it is recommended to apply the latest patch (version 2.16.0) provided by Apache after appropriate testing.***
- Run all systems and services as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.

December 13 – RECOMMENDATIONS:

- Run the "Log4Shell" Vulnerability Tester provided by Huntress to test whether your applications are vulnerable to CVE-2021-44228 (please see references for the *Huntress* link).
- Check the *GitHub* repository listed in the reference section to see all the Security Advisories & Bulletins related to CVE-2021-44228, which include applications affected, version numbers, and the associated patches that should be implemented if you have the affected version in your environment.

For more information, please contact:

CISA, (888)282-0870

Multi-State Information Sharing and Analysis Center (MS-ISAC)
31 Tech Valley Drive,
East Greenbush, NY 12061
24x7 Security Operations Center, SOC@cisecurity.org
1-866-787-4722