The Apache Log4j Security Vulnerability

Critical Steps to Take Now

Take an outside-in approach to identify your impact and exploitability.

STEPS	ACTIONS
1. Scan external surface areas in entirety to itemize vulnerable hosts.	▪ Scan COLOs, AWS, or any cloud provider in your tech stack ▪ Notify your security vendor and ask if a plugin is available
2. Identify which Java codebases have dependencies on Log4j.	▪ Utilize your Software Composition Analysis (SCA) scanning solution ▪ Ensure your scans report both direct and transitive dependencies ▪ Make sure your solution alerts you to any instance of Log4j in your applications ▪ Notify your SCA vendor if you are unsure ▪ Use freely available scanning tools such as Code Aware for Log4j if no SCA tool is in place.
3. Run a grep.	▪ Run a grep command at minimal ▪ Search across all Java codebases looking for log4j*. jar, or log4j-api-*.jar and log4j- core-*.jar
4. Upgrade your dependencies to Log4j 2.16.0.	▪ If you're unable to upgrade, use one of several approved Apache workarounds
5. Check for any and all exploits, new and old (given this opportunity).	▪ Run scans for critical exploits such as old versions of OpenSSL, Apache Struts 2, and others ▪ Create a culture now to scan for issues early and often in your organization

Continued on next page

STEPS	ACTIONS
6. Notify your customers.	▪ Alert them to the actions you are taking to mitigate risk on impacted systems/applications ▪ Let customers know when and how often you will update them on progress and actions
7. Build a remediation plan.	▪ Assemble your team ▪ Define and establish all remediation steps ▪ Know your assets and applications ▪ Communicate with and update stakeholders and all team members ▪ Execute on your plan
8. Establish continuous open source scanning best practices.	▪ If you are not already continuously scanning, enable quickly ▪ If no SCA open source scanning solution is in place, there are solutions available such as Code Insight ▪ Implement an end-to-end solution that discovers security and open source license issues
9. Additional upgrade considerations and thoughts.	▪ If you are on Log4j 2.x, upgrade to Log4j 2.16.0, even if you already upgraded to Log4j 2.15.0 ▪ If you are on Log4j 1.x, start planning for upgrading to Log4j 2.16.0 as soon as you can (this is a more difficult task as there are downstream dependencies with other Java frameworks like Spring) ▪ Expect the target release of Log4j 2.x to change over time, so plan on likelihood of Log4j 2.17.0+ of OpenSSL, Apache Struts 2, and others

Revenera provides the enabling technology to take products to market fast, unlock the value of your IP and accelerate revenue growth—from the edge to the cloud. **www.revenera.com**

Copyright © 2021 Revenera LLC. All other brand and product names mentioned herein may be the trademarks and registered trademarks of their respective owners. | 829_SCA_Log4jGuide