January 3, 2022

Updated Apache Log4j Vulnerability Guidance

As of January 3, 2022, all ADOs using Log4j (2.x and 1.x) must upgrade to 2.17.1 as soon as possible. In the event where the Log4j is attached to a vendor-supplied application, then CISA-published mitigations must be in place until the upgrade is applied.

Background: On December 28, CISA guidance has changed, requiring Log4j 2.17.1 (Java 8), 2.12.4 (Java 7) and 2.3.2 (Java 6). This is in accord to guidance from CISA (https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance) and in compliance to BOD 22-01 (https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

What if I can't patch or I'm waiting for a vendor to release the patch for their applications?
If applying the log4j patch is not an option, you have the following options to mitigate the vulnerability.

- Disable Log4j library. Disabling software using the Log4j library is an effective measure, favoring controlled downtime over adversary-caused issues.
- Disable JNDI lookups or disable remote codebases. This option, while effective, may involve developer work and could impact functionality.
- Disconnect affected stacks. Solution stacks not connected to agency networks pose a dramatically lower risk from attack. Consider temporarily disconnecting the stack from agency networks.
- Isolate the system. Create a "vulnerable network" VLAN and segment the solution stack from the rest of the enterprise network.
- Deploy a properly configured Web Application Firewall (WAF) in front of the solution stack. Deploying a WAF is an important, but incomplete, solution. While threat actors will be able to bypass this mitigation, the reduction in alerting will allow an agency SOC to focus on a smaller set.

If you need additional information or clarification, please work with your internal ADO team, HIDS Cloud Support Manager (CSM), the HIDS Security Team, or CMS Information System Security Officer (ISSO).