CyberTools and the Log4j vulnerability

2021-12-14

CyberTools found and removed the only instance of Log4j on its servers on 2021-12-14. The Log4j vulnerability has been reported widely by the tech and consumer press. Our steps were:

1. Refresh snapshots of CyberTools root and executable AWS volumes for fast recovery in the case of breach.

2. Stop the web server on one of the CyberTools shadow servers. A shadow server is a hot replace for a live server if the live server fails. This ensures that at least this one server cannot be compromised by the Log4j vulnerability. It does increase the hot replacement time.

3. CyberTools staff removed log4j from the one package that used log4j on all servers.

4. We hired an outside consultant to review our mitigation steps.