athenahealth

Take immediate action to address critical vulnerability

This message applies to all athenaPractice customers live on v12.3.1 and higher and athenaFlow customers live on v9.12.1 and higher.

The Apache Software Foundation has released an **emergency security advisory** to address a remote code execution vulnerability potentially affecting Log4j versions 2.0-beta9 to 2.14.1. The Log4j is a widely used logging library and is used in the athenaPractice and athenaFlow versions referenced above. A remote hacker could exploit this vulnerability to take control of an affected system (i.e. bad actors gaining access to your environment). This issue is being tracked as CVE-2021-44228 and by the monikers Log4Shell or LogJam.

We strongly advise you to take steps to mitigate this vulnerability *as soon as possible*. Detailed instructions can be found in Knowledge Article 000105175 located on the Success Community.

If you have questions or need assistance, reach out to our Support Center or your VAR (if applicable).