1601 S MoPac Expy, Suite 100
Austin, TX 78746
(P) +1 (512) 347-9300
www.lifesize.com

Apache Log4j2 (CVE-2021-44228)

Lifesize is aware of the vulnerability related to the Apache Foundation Log4j library. This vulnerability could allow an attacker who can control log messages or log message parameters to execute arbitrary code loaded from LDAP, authentication, servers.

Apache Log4j and the vulnerability

Apache Log4j is a Java-based logging utility. A code execution vulnerability has been discovered in Log4j. This application is prone to this vulnerability when message lookup substitution is enabled.

What has Lifesize done?

Upon becoming aware of this vulnerability, on December 10th, 2021, our Security Operations Center has been continuously monitoring our environment and log details for suspicious behavior.

- After receiving additional details about the scan signature our SOC began investigations dating from December 1st, 2021, to present and no event has been found
- Our Engineers also completed internal reviews and validated that our systems do not use the vulnerable Apache Log4j library
- Team members have also confirmed that third party solutions we leverage were either not impacted or have taken the necessary steps to remediate the issue within their systems

What remediation steps need to be taken?

Lifesize teams have confirmed that there are no remediation steps needed for our CCaaS, VCaaS, and on-premise solutions.

Lifesize continues its commitments to protection and security without comprise. To learn more about our products and services please visit us at https://www.lifesize.com.