StarLeaf statement in reference to the Log4j vulnerability

On 10 December 2021, StarLeaf became aware of the Log4j vulnerability (CVE-2021-44228) which permits unauthenticated remote code execution (RCE) on any Java applications running a vulnerable version of Apache's Log4j 2 [1]. StarLeaf has investigated this issue across two key services: (1) the StarLeaf global video service and (2) the StarLeaf Standby service.

Neither service uses the Log4j component.

Where StarLeaf does use the Log4j component, it is running on an internal, protected network which is unreachable from the outside. StarLeaf Engineering teams confirm that no tampering or exploitation has taken place.

For all questions and concerns on this topic, please reach out to infosec@starleaf.com. Security and privacy remain one of the highest priorities at StarLeaf, and we continue to monitor this situation. Any further updates about this issue will be posted to this blog site.

References

Easterly, J. (2021, December 11). Statement from CISA Director Easterly on Log4j Vulnerability. Cybersecurity and Infrastructure Security Agency. Retrieved from https://www.cisa.gov/news/2021/12/11/statement-cisa-director-easterly-log4j-vulnerability

Nist.gov. (2021, December 10). CVE-2021-44228 Detail. National Vulnerability Database. Retrieved from https://nvd.nist.gov/vuln/detail/CVE-2021-44228

Footnotes

[1] The Log4j vulnerability (CVE-2021-44228) permits unauthenticated remote code execution (RCE) on any Java applications running a vulnerable version of Apache's Log4j 2. It poses a severe risk to those using this version, because it can permit an unauthorized access or complete control over systems when exploited correctly.