Collaborative Discussion 2: The Pros and cons of logging – The impact of log4j

Initial post:

Managing the security of information systems is a complex task that is becoming more challenging due to the increasing number of security threats. Security analysts must handle log data from various sources to identify suspicious activity. However, performing comprehensive log analysis is still a manual process that does not scale well (Ekelhart et al. 2019).

According to Smith (2022), monitoring logs is crucial for organisations to detect unusual behaviour, investigate security issues, maintain system integrity, help security teams quickly resolve incidents, and ensure regulatory compliance. By recording every action, logging reduces risks and helps identify potential security breaches.

Log4j 2 is a popular logging framework that logs messages from software and can create simple logs and execute commands for advanced logging (Berger, 2021). System administrators rely on records to monitor and analyse system activity. However, it is essential to protect them to avoid potential security risks. As highlighted by NCSC (2021), Log4shell is a vulnerability in the logging program Log4j that poses a significant threat to organisations worldwide.

Kapsamer (2023) states that logs must be protected from malicious attacks since they might be altered or deleted. As Berger (2021) recommended, organisations using Log4j 2 should update their applications and infrastructure immediately to protect against Log4Shell vulnerability.

References

- Ekelhart, A., Kiesling, E. and Kurniawan, K. (2019). Taming the logs - Vocabularies for semantic security analysis. *Procedia Computer Science*, 137, pp.109–119. doi:https://doi.org/10.1016/j.procs.2018.09.011.
- Smith, A. (2022). *Log Monitoring: A Complete Guide*. [online] Available at: https://www.defense.com/blog/what-is-log-monitoring [Accessed 28 Nov. 2023].
- Berger, A. (2021). *What is Log4Shell? The Log4j vulnerability explained (and what to do about it)*. [online] Dynatrace news. Available at: https://www.dynatrace.com/news/blog/what-is-log4shell/?utm_source=google&utm_medium=cpc&utm_term=log4j%20vulnerability%20explained&utm_campaign=uk-application-security&utm_content=none [Accessed 28 Nov. 2023].
- NCSC (2021). *Log4j vulnerability - what everyone needs to know*. [online] www.ncsc.gov.uk. Available at: https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know.
- Dörre, F. & Ottenhues, A. (N.D.). *Secure Logging in between Theory and Practice: Security Analysis of the Implementation of Forward Secure Log Sealing in Journald*. [online] Available at: https://eprint.iacr.org/2023/867.pdf [Accessed 28 Nov. 2023].
- Kapsamer, R. (2023). *The Hidden Threat to Your SecOps: Tampered Log Data*. [online] Tributech. Available at: https://www.tributech.io/blog/log-data-integrity [Accessed 28 Nov. 2023].