**The Pros and Cons of Logging**

**Introduction**

In 2021, the Log4j vulnerability was given a CVSS score of 10, the highest a vulnerability can achieve. Malicious actors had exploited it for at least two years before researchers identified it (Berger, 2024). The software's prolific nature and the ease with which it was exploited have highlighted the need for robust security measures across IT infrastructure, including logging tools. This post will cover the benefits of logging for security analysis and the potential risks associated with log-related exploits.

**Logging for security analysis**

Logging is the term for collecting data within an IT system, such as running processes, software failures, and user activities and storing it in files known as “logs” (Sacred Heart University, N.D.). Logs are a necessary tool for a security analyst, providing valuable information such as which user clicked a suspect link or when a configuration change may have occurred (NCSC, 2018).

The benefits of logging tools were highlighted during the SolarWinds attack. FireEye observed in its logs that one of its employees had two phones registered to their name. This triggered an investigation, which led to the company discovering they were victims of the attack (Sharwood, 2021). FireEye’s ability to audit its logs and, therefore, maintain incident control highlights the importance of logging and its ability to assist a security analyst.

**Log-related exploits**

However, as with all areas of technology, logging has risks. If data is not adequately processed, a malicious payload may be stored server-side, causing persistent harm to an application (Pan, 2022). An example is the Log4j vulnerability, which allowed a hostile user to execute arbitrary code in LDAP servers (NIST, 2021).

Sanitising user input is imperative to avoid forged log files and the leakage of sensitive data (Mohindra, 2024). Using a framework such as NIST SP 800-53 is also encouraged. The Audit and Accountability (AU) family of controls details the protection of auditing and logging tools from unauthorised access, modification, and deletion (NIST, 2020). This will ensure that rather than increasing the attack surface for a hostile actor, logging remains a valuable tool for the security analyst.

**Conclusion**

Logging provides valuable insights into an IT system's events. However, as Log4j demonstrated, such tools still have vulnerabilities. Careful configuration and implementation, including sanitising data and using a framework, will prevent forged logs and the leakage of sensitive data, ensuring logging will remain valuable for a security analyst.

**References**

* Berger, A. (2024) What is Log4Shell? The Log4j vulnerability explained (and what to do about it). Available from: <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&gclid=CjwKCAjwiuuRBhBvEiwAFXKaNJd3hLzYlujXuVbTIP63_IioBFvzAYOePxfft2D6ded7EXfaTu4j4BoCrHAQAvD_BwE&gclsrc=aw.ds> [Accessed 22 August 2024].
* Mohindra, D. (2024) IDS03-J. Do not log unsanitized user input. Available from: <https://wiki.sei.cmu.edu/confluence/display/java/IDS03-J.+Do+not+log+unsanitized+user+input> [Accessed 22 August 2024].
* NCSC. (2018) Introduction to logging for security purposes. Available from: <https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes> [Accessed 21 August 2024].
* NIST. (2020) *Security and Privacy Controls for Information Systems and Organizations.* DOI: https://doi.org/10.6028/NIST.SP.800-53r5
* NIST. (2021) CVE-2021-44228 Detail. Available from: <https://nvd.nist.gov/vuln/detail/CVE-2021-44228> [Accessed 22 August 2024].
* Pan, Z., Chen, Y., Chen, Y., Shen, Y. & Li, Y. (2022) LogInjector: Detecting Web Application Log Injection Vulnerabilities. *Applied sciences* 12 (15): 7681-. DOI:10.3390/app12157681
* Sacred Heart University. (N.D.) Cybersecurity And The Importance of Log Files. Available from: <https://www.sacredheart.edu/academics/colleges--schools/school-of-computer-science--engineering/computer-science--cybersecurity-blog/cybersecurity-and-the-importance-of-log-files/#:~:text=In%20the%20world%20of%20cybersecurity,login%20and%20current%20login%20status>. [Accessed 21 August 2024].
* Sharwood, S. (2021) Microsoft says it found 1,000-plus developers’ fingerprints on the SolarWinds attack. Available from: <https://www.theregister.com/2021/02/15/solarwinds_microsoft_fireeye_analysis/> [Accessed 24 August 2024].