Network Security - Module 3

The Pros and Cons of logging - The impact of Log4j

Collaborative Discussion 2

Initial Post

Logging

Logging plays an important part in businesses and systems, therefore, it is paramount that the integrity of logs are maintained. According to Zeng et al (2016), many standards and regulations for organizations to carry out their daily operations require logging mechanisms to be in place. Now, more than ever, has become an important time to be able to produce accurate and readable logs, especially during auditing and forensic investigations. The process of logging in operating systems has become a crucial element of their respective kernels (Zeng et al. 2016).

What is log4j?

It can be said that log4j is a multi pronged logging framework, multi pronged because it is able to do more than just log messages from software, it can also execute commands and communicate with internal directory services and other sources (Berger, 2021). Using the ${variable} format, log4j can override previous logs and execute in the log4j 2 version. This exploit would allow an attacker to carry out a remote code execution, Denial-of-service attack and cause data leakage (Berger, 2021).

Issues of logging for security analysis

Logs are extremely helpful for security analysis but there are also many issues that are increasing the difficulty of analysis, and one of those issues is pure volume from an increase in data. According to Ekelhart et al (2018), failure to detect and respond to incidents due to the inability to perform manual analysis on such a scale is an issue for organizations.

Issues of log-related exploits

An issue with log related exploits may be that companies who are using third party products may be reliant on that third party to ensure that they have updated and patched sufficiently. If a Software bill of materials (SBOM) has not been produced, then it is possible that users of the third party products will be open to exploits.

To conclude, due to the wide variety of log types and the vast amount of data generated, it has become clear that an organization should outline which type of logs they wish to utilize and create a framework for how that data is structured and what type of architecture they are pulling logs from. According to NIST (2006), active testing and validation can be performed via a representative sampling of the system by carrying out an activity and then checking if the logs capture that particular activity correctly.

References

Berger, A. (2021) What is Log4hell? 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 14 February 2023].

Ekelhart, A. et al (2018) Taming the logs - Vocabularies for semantic security analysis. *Procedia Computer Science* (137)

NIST. (2006) Guide to computer security log management: *NIST 800-92.* Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-92.pdf [Accessed on 14th February 2023]

Zeng, L., Xiao, Y., Chen, H., Sun, B. and Han, W., (2016). Computer operating system logging and security issues: a survey. *Security and communication networks*, *9*(17), pp.4804-4821.