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

Initial Post

by Gokul Kurunthasalam - Monday, 18 July 2022, 3:18 PM
Number of replies: 1

Pros:

Log files offer a crucial audit trail that may be used to track activity within an IT infrastructure, spot policy violations, track down fraudulent or anomalous activity, and draw attention to security concerns. The Center for Internet Security counts log management as one of its major security controls because it recognises the significance of the security log management process. The Federal Information Security Modernization Act, ISO 27001, HIPAA, Sarbanes-Oxley Act, Gramm-Leach-Bliley Act, National Industrial Security Program Operating Manual, and PCI DSS are just a few of the regulations and standards that require log management for compliance and reporting.

Security teams can use logs to investigate and assess where an attack is coming from or coming from, determine how an attack has damaged IT resources, and detect and respond to indicators of compromise since they provide data of what has happened and what is happening.

Cons:

It is difficult to manage security logs. A tiny business nonetheless produces a lot of loggable data, even if it just records the events that pertain to the most crucial metrics. Large businesses can generate hundreds of gigabytes of log data.

Logs need to be normalised because they originate from numerous endpoints and have diverse sources, formats, and formats. The goal is to organise the data in a consistent manner that makes it simple to search, compare, and read.

Due to the ever-changing multitude of log formats, log types, and log sources, maintenance expenses might soar to unmanageable heights that the project is frequently killed. To add to, modify, or fix the solution, you will need a crew with exceptional skills.

Impact of Apache Log4j vulnerability:

The Apache Log4j vulnerability (CVE-2021-44228), which poses a high risk and challenging situation for enterprises, has affected more than 44% of corporate networks globally. The software industry has been damaged by the log4j vulnerabilities' extensive effects because the disclosure severely affected hundreds of Java programmes.

References:

Wongthai, W., van Moorsel, A. (2016). Quality Analysis of Logging System Components in the Cloud. In: Kim, K., Joukov, N. (eds) Information Science and Applications (ICISA) 2016. Lecture Notes in Electrical Engineering, vol 376. Springer, Singapore. https://doi.org/10.1007/978-981-10-0557-2_64

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