SBOMs Are the Bomb

Wendy Edwards

Are You Vulnerable?

Lots of CVEs

Lots of software projects

Finding a needle in a haystack?




Project Idea

- Use PALM to read information about software vulnerabilities and provide additional data that would allow software projects to be automatically scanned

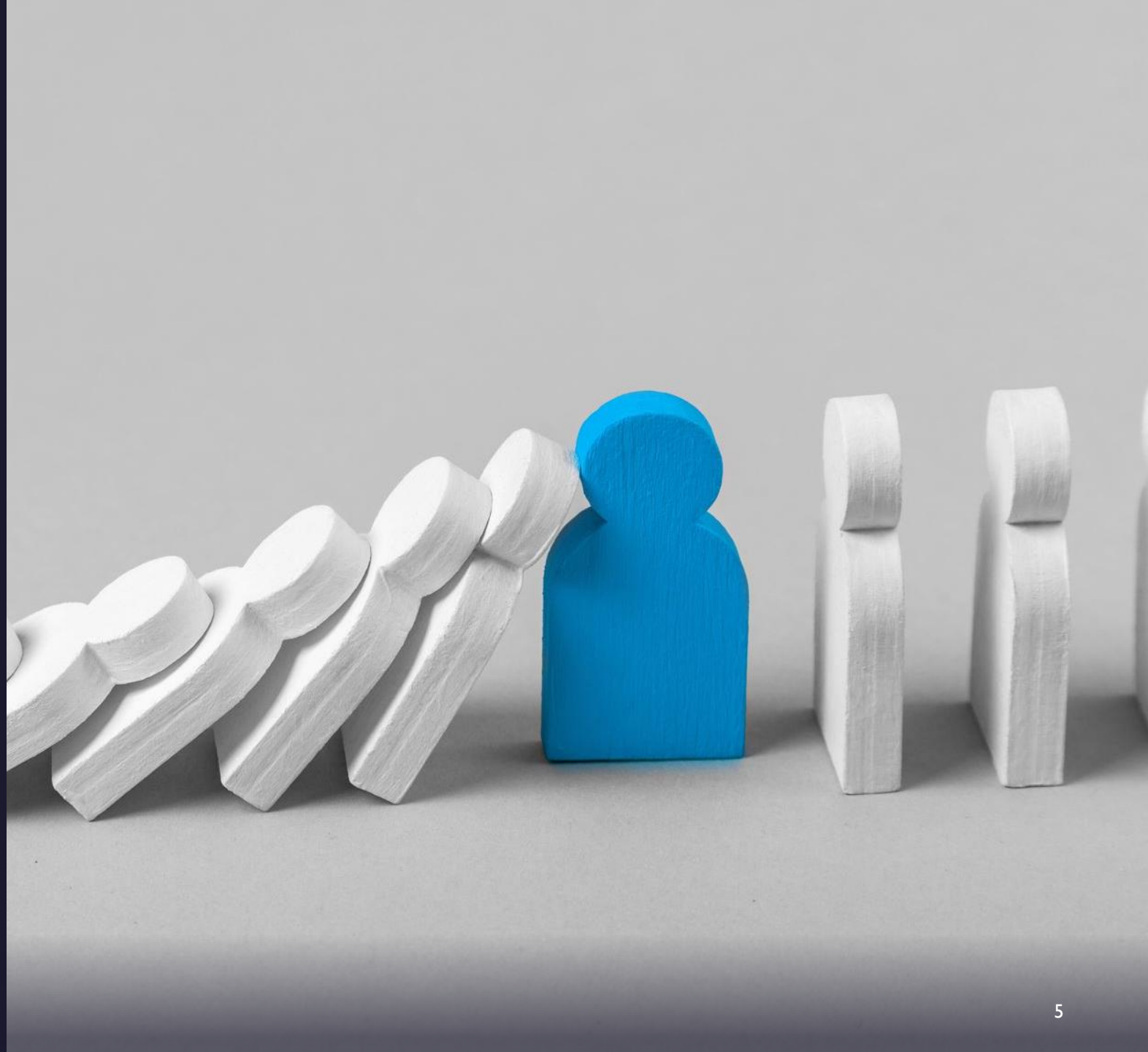
Log4J bug in 2021 (CVE-2021-44832)

- Version information looked like this:
  `"Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack...."`
- Not conducive to scanning
- PALM generated list of affected Log4J versions
- Now we can scan!

More potential

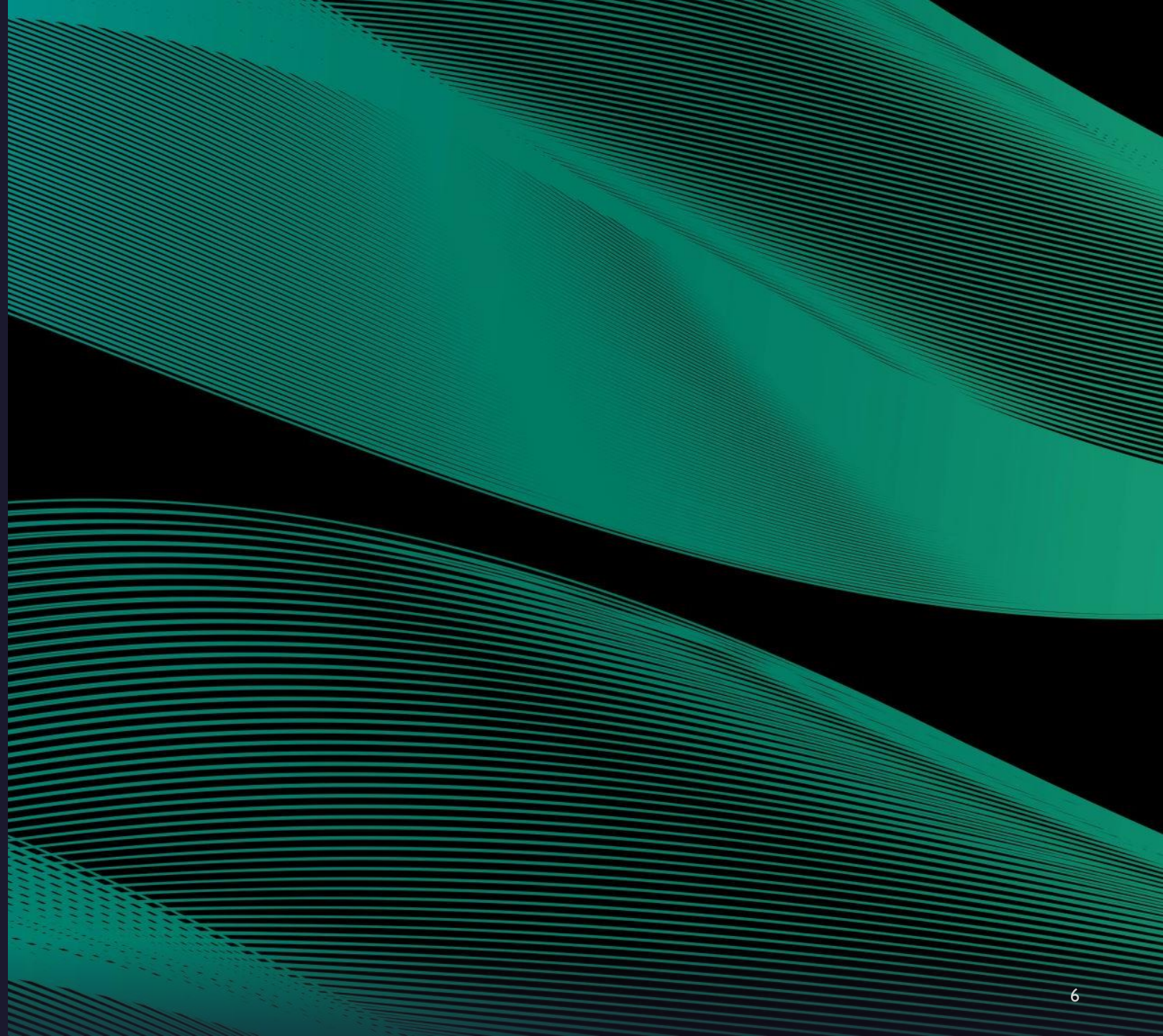
PALM could help to generate CVE JSON files from text descriptions

Could handle minor differences in text that would have made automatic scanning more difficult, e.g. “Log4J2” vs “Log4J 2”



"When you feel lost, remember that you are not alone. Everyone feels lost sometimes. The important thing is to keep moving forward and never give up on yourself."

- Google PALM, when given the prompt “Please generate an inspirational message.”



Summary

This project read data from MITREs CVE and used Google PALM to generate additional information to make it easier to automatically scan software for vulnerabilities.

Thank You

Wendy Edwards

mrscake@gmail.com

https://www.linkedin.com/in/wendy-edwards-a45a481/