LOG4SHELL EXPLOIT

REMOTE CODE EXECUTION
CVE-2021-44228

Nicholas Jacob

University of Advancing Technology

June 12, 2022

WHAT IS LOG4J

- Open-source software by Apache Software Foundation
- Records Events
  - Errors
  - Routine System Operations
- Communicates diagnostic messages to Admins and Users
- Examples: 404 Error, Minecraft servers log memory used and console commands entered

HOW LOG4SHELL EXPLOIT WORKS

- Log4j feature allows log messages to be specially formatted by users
- Messages can be formatted to contain variables
  - Variables can be requested from separate servers
- Variables are translated before being logged
- Requested variable can be in the form of code

WHY ITS SO BAD- CVSS SCORE: 10.0 CRITICAL

- Log4j's widespread use
- Low complexity
- No privileges required
- No user interaction required
- New vulnerabilities followed as a result

RELATED VULNERABILITIES

- CVE-2021-45105
- CVE-2021-45046
- CVE-2021-44832
- CVE-2021-4104
- CVE-2022-23302
- CVE-2022-23305
- CVE-2022-23307

Log4j vulnerabilities dated before Log4Shell

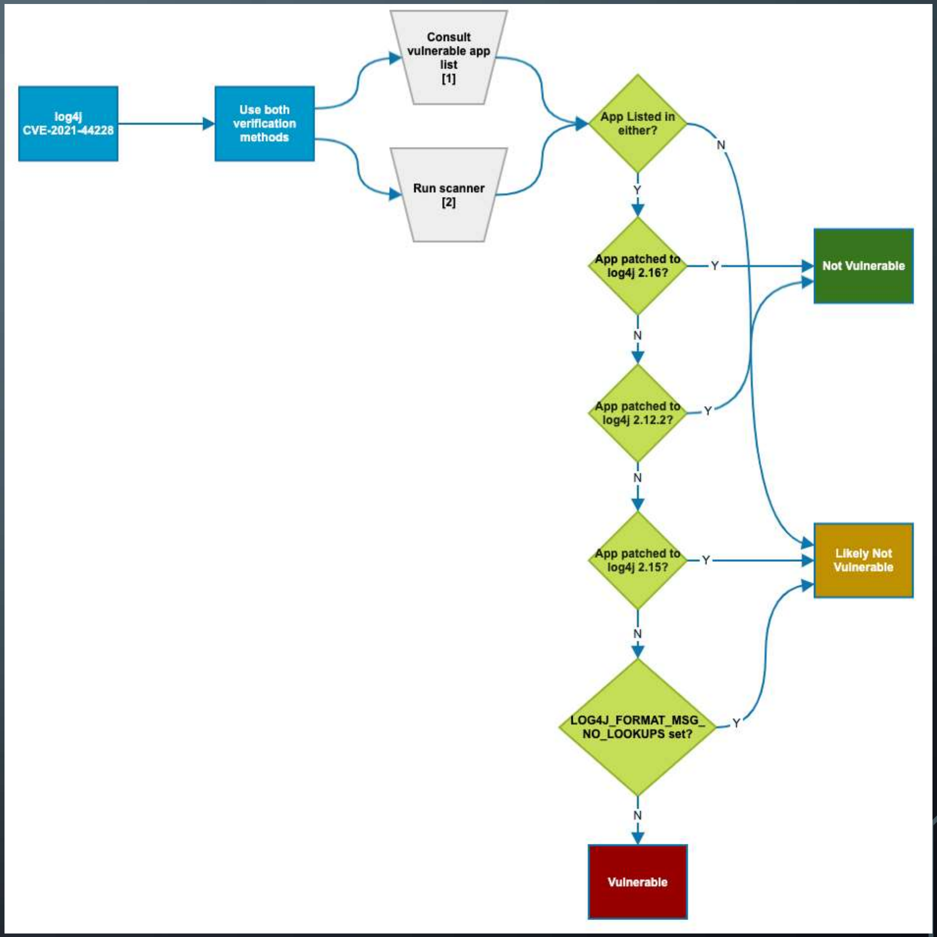
- CVE-2020-9493
- CVE-2020-9488
- CVE-2019-17571
- CVE-2017-5645

TECH USING LOG4J

- Minecraft
- VMWare: Various Products
- Apple iCloud
- AWS
- Adobe ColdFusion
- Cisco: Various Products
- Apache: Various Products
- F-Secure: Various Products
- Broadcom: Various Products
- Fortinet
- FortiGuard
- IBM
- Okta

ACTIONS

- Follow CISA flow chart to determine vulnerability
- Update all vulnerable apps
- Continue to watch for future app updates
- Stay informed on new exploits



log4j CVE-2021-44228

Use both verification methods

Consult vulnerable app list [1]

Run scanner [2]

App Listed in either?

App patched to log4j 2.16?

App patched to log4j 2.12.2?

App patched to log4j 2.15?

LOG4J_FORMAT_MSG_NO_LOOKUPS set?

Not Vulnerable

Likely Not Vulnerable

Vulnerable

REFERENCES

Apache " LOG4J : Security vulnerabilities. CVE Details. (n.d.). Retrieved June 9, 2022, from https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-37215/Apache-Log4j.html

Apache LOG4J vulnerability guidance. CISA. (n.d.). Retrieved June 9, 2022, from https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

Howard, T. (2021, December 12). *Log4Shell Explained*. Cynet XDR | Autonomous Breach Protection. Retrieved June 9, 2022, from https://www.cynet.com/attack-techniques-hands-on/log4shell-explained/

Nath, O. (2022, February 15). *Log4j Flaw: Top 10 Affected Vendors and Best Solutions to Mitigate Exploitations*. Toolbox.com. Retrieved June 9, 2022, from https://www.toolbox.com/it-security/vulnerability-management/articles/log4j-flaw-top-10-affected-vendors-and-best-solutions-to-mitigate-exploitations/

NIST. (2021, December 10). *CVE-2021-44228*. NVD. Retrieved June 9, 2022, from https://nvd.nist.gov/vuln/detail/CVE-2021-44228#vulnCurrentDescriptionTitle

Torres-Arias, S. (2021, December 22). *What is Log4j? A cybersecurity expert explains the latest internet vulnerability, how bad it is and what's at stake*. The Conversation. Retrieved June 9, 2022, from https://theconversation.com/what-is-log4j-a-cybersecurity-expert-explains-the-latest-internet-vulnerability-how-bad-it-is-and-whats-at-stake-173896