T2021_22 Tip to protect against Log4j Exploitation (21st December 2021)

What is the Apache Log4j Vulnerability?

A series of vulnerabilities were recently discovered in the popular Java-based logging library "Log4j" which resulted in the exploitation of a critical remote code execution (RCE) vulnerability (CVE-2021-44228) by various malicious actors. This exploit allowed unauthorized attackers to remotely execute code on a server. Exploitation can be successful even if the software accepting input is not written in Java because such software is able to pass malicious data to other systems that are written in Java.

How to protect against Log4j Exploitation:

Organisations are urged to review and monitor the Apache Log4j Security Vulnerabilities webpage (https://logging.apache.org/log4j/2.x/security.html) for updates and guidance on the issue. To protect against Log4j exploitations, it is advised to:

- Identify all internet-facing assets that allow data inputs and that utilize the Log4j Java library. Verification methods can be found at:
    - CISA Log4j (CVE-2021-44228) Mitigation Guidance: https://github.com/cisagov/log4j-affected-db
    - CVE-2021-44228_scanner: https://github.com/CERTCC/CVE-2021- 44228_scanner
- Identify all assets that use the Log4j library.
- Update or isolate affected assets.
- For all solution stacks containing software that were identified as affected: assume compromise, identify potential post-exploit activities, thoroughly investigate for signs of malicious activity, and immediately apply patches where necessary to internet- facing assets, mission critical systems and networked servers. Mitigation measures can be found at: https://www.cisa.gov/uscert/ed-22-02-apache-log4j-recommended- mitigation-measures
- Monitor for odd traffic patterns (e.g., JDNI LDAP/RMI outbound traffic, DMZ systems initiating outbound connections).

The Guyana National CIRT recommends that users and administrators review these recommendations and implement them where necessary.

Reference

- Apache Log4j Vulnerability Guidance. (2021, December). Retrieved from Cybersecurity Infrastructure Security Agency: https://www.cisa.gov/uscert/apache- log4j-vulnerability-guidance

- CISA (2021, December). EMERGENCY DIRECTIVE 22-02 MITIGATE APACHIE LOG 4J VULNERABILITY. Retrieved from Cybersecurity and Infrastructure Security Agency: https://www.cisa.gov/emergency-directive-22-02