Log4j2 Vulnerability
RCE and DoS in Apache Java logging library
CVEs: CVE-2021-44228 CVE-2021-45046 CVE-2021-45105 CVE-2021-44832

A 0-day exploit was discovered on a popular Java library Log4j2 that can result in a Remote Code Execution (RCE). This is a widely deployed library, and while systems protected by Fortinet Security Fabric are secured by the protections below, all systems need to upgrade ASAP as this is 10.0 severity. Due to the high visibility and attention, subsequent vulnerabilities have since emerged.

Background
The Log4j2 is a Java-based logging utility that is part of the Apache Software. Detailed background is available in the Fortinet Blog: https://www.fortinet.com/blog/threat-research/critical-apache-log4j-log4shell-vulnerability-what-you-need-to-know

If you are looking for information pertaining to Fortinet products impacted by this vulnerability, refer to: https://www.fortiguard.com/psirt/FG-IR-21-245?utm_source=blog&utm_campaign=blog

And, for more technical information pertaining to each vulnerability, please refer to the FortiGuard Threat Signals:


Announced
On Dec 9, a 0-day was posted on Twitter with a PoC posted in GitHub. On Dec 10, several security-related websites picked up the vulnerability and released an article.

Latest Developments
Jun 27, 2022: Over 6 months later, stories of Log4j2 exploits continue to be published on near-daily basis and FortiGuard Labs continues to see active exploitation attempts. On a single day (Jun 14, 2022), FortiGuard IPS blocked over 50,000 exploits.

Cyber Kill Chain

Incident Response (Security Operations)
To help customers identify and protect vulnerable, FortiAnalyzer, FortiDBR and FortiSASE updates are available to raise alerts and escalate to incident response:

Incident Response (Security Operations)

- Threat Hunting
  - FortiAnalyzer
    - Threat Hunting - 1.00041

  - FortiSIEM
    - Threat Hunting - 6.0+.

  - FortiSOAR
    - Threat Hunting - 6.0+.

Additional Resources
- CISA

- US CERT

- Apache
  - https://logging.apache.org/log4j/2.x/security.html

- Threat Signal