>_Log4Shell

Exploiting our demo app

Unconference| 22-05

Log4Shell
Definition

allows an attacker to remotely run malicious code – potentially unauthenticated
RCE = Remote Code Execution

API that provides naming and directory functionality e.g., DNS or LDAP lookups,
JNDI = Java Naming and Directoy Interface

"Unauthenticated RCE 0-day exploit using JNDI in log4j"

refers to the fact that the owner has only just learned of the flaw – which means they have “0 days” to fix it

Log4Shell

Exploiting playbook