Log4Shell

Tổng quan

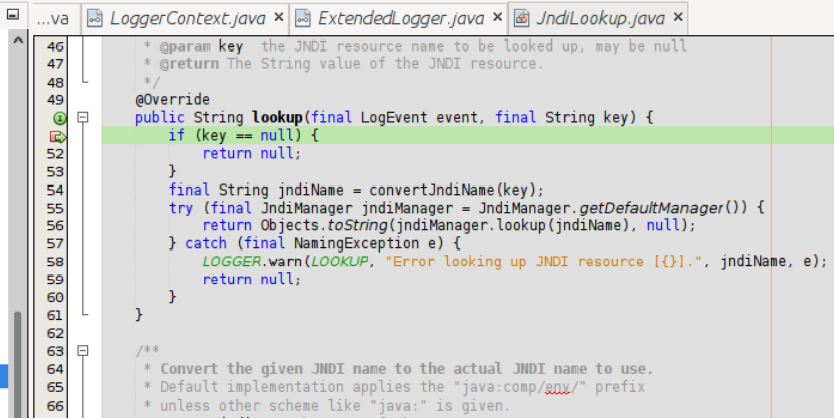
Log4Shell được tìm thấy trong file log4j, tập tin ghi lại nhật ký hoạt động (log) của các ứng dụng thường dùng để truy vết lỗi. Hầu hết các hệ thống bảo mật đều có một file nhật ký như vậy. Log4j thường nằm trong phần mã nguồn mở do apache phát hành.

Kẻ tấn công có thể truy cập vào các máy chủ web mà không cần mật khẩu, từ đó có thể thâm nhập vào các mạng nội bộ đánh cắp dữ liệu có giá trị, cài đặt phần mềm độc hại…

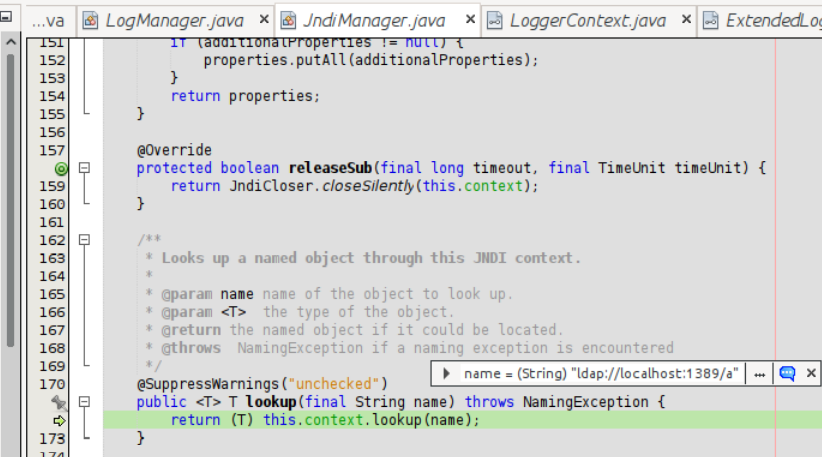
Luồng thực thi

Kẻ tấn công sẽ gửi 1 input cho ứng dụng chứa lỗ hổng, kích hoạt code ghi log.

Thư viện log4j2 sẽ phân tích cú pháp trên, nếu nhận yêu cầu có chứa Slookup jndi thì sẽ gọi đến phương thức JnduLookup.lookup() và truyền vào đó tham số đường dẫn đến server LDAP.



Phương thức này sẽ gọi đến phương thức JndiManager.lookup() của thư viện JNDI.

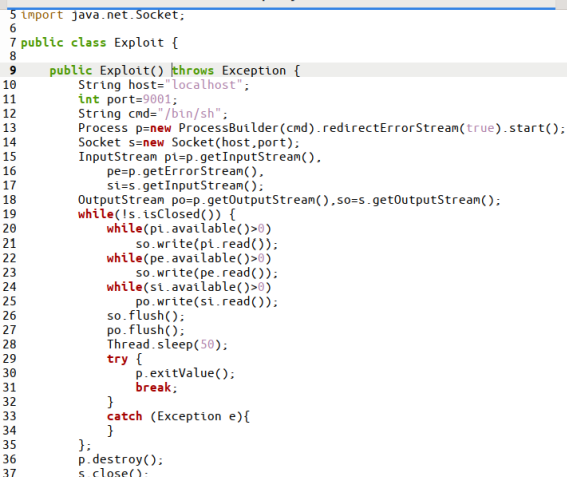


Từ đây, JNDI sẽ truy vấn dến server LDAP, lấy về đối tượng được truy vấn,

phân tích đối tượng. JNDI nhận thấy có attribute “javaCodeBase” và

“javaFactory” do đó sẽ thực hiện download đối tượng tại đường dẫn

“javaCodeBase/javaFactory”

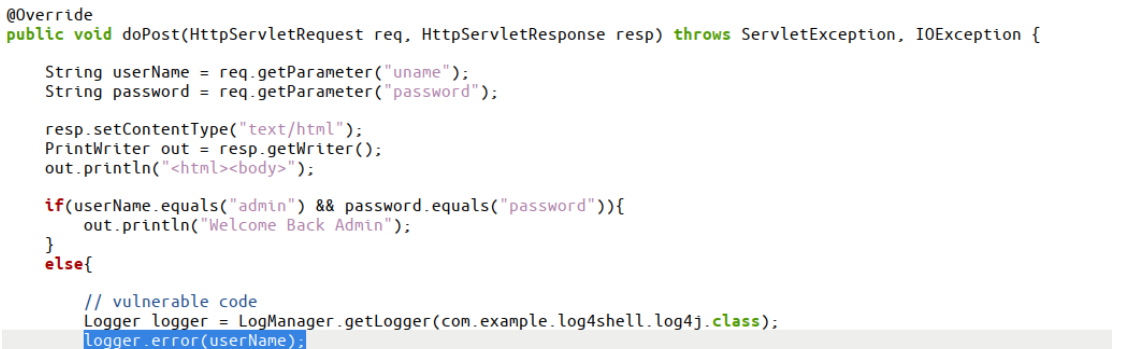


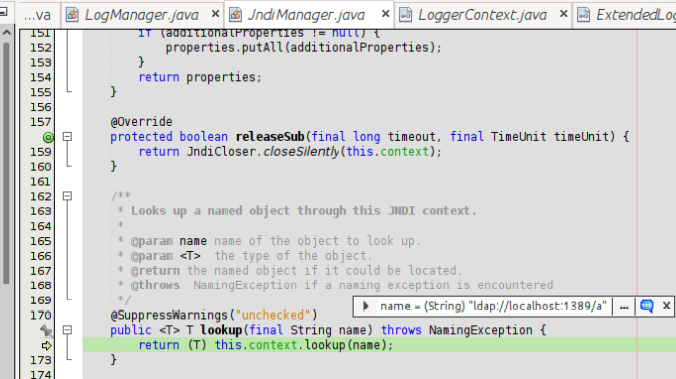
Trong version log4j 2.14.1, không hề có đoạn code ngăn chặn việc sử dụng jndi để

lấy dữ liệu từ bên ngoài cũng như việc kiểm tra địa chỉ server LDAP. Cụ thể, từ

đoạn code thực hiện ghi log

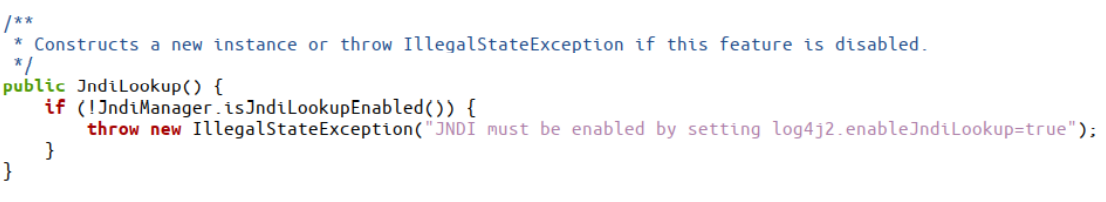
S





Để khắc phục điều này, trong bản cập nhật (version 2.17.0), trong file

“JndiLookup.java” đã được thêm vào đoạn code:



Hoạt động: kiểm tra tính năng “jndi lookup” có được cho phép hay không. Nếu không, lập tức throw (raise) một exception khiến hoạt động lookup bị ngừng lại.