**Log4j 관련 이슈 분석 사항**

**문제 발생**

2013-09-14 released 2.0-beta9

migration : https://blogs.apache.org/logging/entry/apache\_log4j\_2\_0\_beta9

LOG4J2-313 : Add JNDILookup plugin

해당 버전에서 'JNDILookup plugin'를 기존 log4j에 추가함에 있어 보안성 문제가 발생하게 되었다.

**문제 발생 배경**

JNDI는 디렉터리 서비스에서 제공하는 데이터 및 객체를 발견하고 참고하기 위한 자바 API로, 일반적으로 TCP/IP 상에서 디렉터리 서비스를 조회하고 수정하는 응용 프로토콜, 작업 메시징 시스템에 권장되는 객체 저장소인 LDAP 서버를 사용한다는 특징이 존재하였다.

JNDI와 LDAP를 사용하면 간단한 문법인 ${prefix:name}형식을 통해 통신 서버에 접속한 단말을 조종하여 해커가 원하는 악성 코드를 다운로드 받을 수 있도록 조종할 수 있었으며, 이를 통해 원격 조종까지 가능한 RCE(remote code execution) 문제가 발생한다는 취약점이 오랫동안 존재했다는 것이 밝혀졌다.

한마디로 해당 문제가 발생한 버전을 사용하는 사용자가 서버에 접속하기만 해도 해커가 앞서 말한 악성 기술을 활용해 사용자의 컴퓨터에 존재하는 모든 정보를 훔칠 수 있을 정도로 심각한 문제가 사람들이 일반적으로 사용하는 기술에 존재하였던 것이다.

**문제 대응 방안**

따라서 웹에서는 몇 가지 대응 방안이 제시되고 있다.

1. 해당 문제가 발생하는 계기가 된 JndiLookup 클래스를 경로에서 제거하거나

zip -q -d log4j-core-

\*.jarorg/apache/logging/log4j/core/lookup/JndiLookup.class

1. 해커가 사용하는 문법을 웹 방화벽/IPS 수준에서 차단하여 해당 구문을 이용하지 못하도록 하거나

${jndi:lap:/

${jndi:dns:/

${jndi:rmi:/

${jndi:ldaps:/

${jndi:iiop:/

${jndi:http:/

${jndi:nis:/

${jndi:nds:/

${jndi:corba:/

1. 해당 수법을 주로 이용하는 IP를 차단하는 방법을 추천하고 있으며

Log4j 관계자가 발표한 Log4j 2.17.0 버전으로의 패치가 권장되고 있었다.

**추가적으로 발생한 문제**

그러나 JNDI+LDAP를 이용한 문제와 더불어 기존 Log4j 1.2버전에서 사용되었던 JMSAppender에서도 비슷한 취약점이 존재한다는 것이 발견되었으며, 이를 해결하기 위해 JMSAppender를 log4j.xml 등의 설정 파일에서 사용하지 않도록 하거나, 명령어를 통해 직접 JMSAppender를 제거하는 방법이 추천되고 있다. (zip -q -d log4j-\*.jar org/apache/log4j/net/JMSAppender.class)

현재까지 밝혀진 문제점들을 수정한 Log4j 2.17.1버전이 공개되었고, 해당 버전으로 패치가 권장되고 있지만, 아직까지도 숨겨진 문제점들이 밝혀지고 있는 사항이니 주기적으로 관련 소식을 찾아 대처하는 자세를 가지는 것이 권장되고 있다.