Q&A 형식으로 알아보는 log4j 보안 취약점 대응 가이드

- 목 차 -

2021.12

[대상 : 취약점 조치를 담당하는 **시스템 관리자**]

작성된 시점까지 확인한 내용을 기반으로 하므로 업데이트될 수 있으며
기업 내부적으로 취약점에 대한 대응 절차를 수립하여 지속적인 관리가 필요합니다

Log4j 취약점을 악용한 침해사고 발생 시 한국인터넷진흥원으로 반드시 신고하시기 바랍니다.

과학기술정보통신부 Ministry of Science and ICT
KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

log4j 취약점 대응 FAQ
(CVE-2021-44228, CVE-2021-45046, CVE-2021-4104)

Q1. log4j가 무엇인가요?

○ log4j의 기능은 웹 서비스 동작 과정에서 일어나는 일련의 모든 기록을 남겨 침해사고 발생 및 이상징후를 점검하기 위해 필수적으로 필요한 기능입니다. 무료로 제공되는 오픈소스 프로그램으로 Java 기반의 모든 어플리케이션에서 사용할 수 있습니다.

Q2. log4j는 어떤 서비스들에 주로 사용되나요?

○ 일반적인 웹 사이트, 쇼핑몰, 그룹웨어 등 Java를 기반으로 한 JVM(Java Virtual Machine) 환경을 사용하는 모든 서비스에서 사용 가능합니다

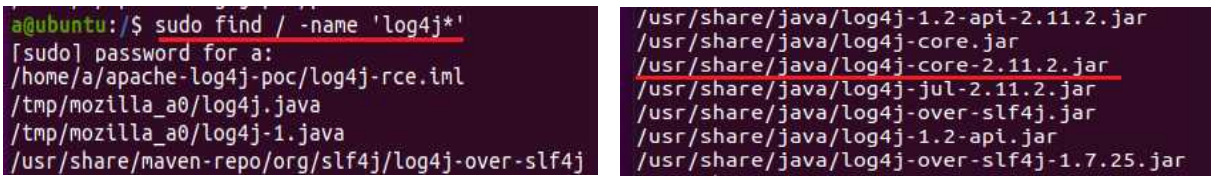
Q3. 취약한 log4j를 사용하고 있는지 어떻게 확인하나요?

○ log4j를 사용하는 제품에 관한 정보는 아래 링크에서 확인할 수 있습니다.

- 상용제품 사용 중인 경우 아래 링크에 접속하여 해당 제조사를 찾아 제조사가 안내하는 방법으로 확인
  * https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

○ log4j 설치 여부 확인(linux)

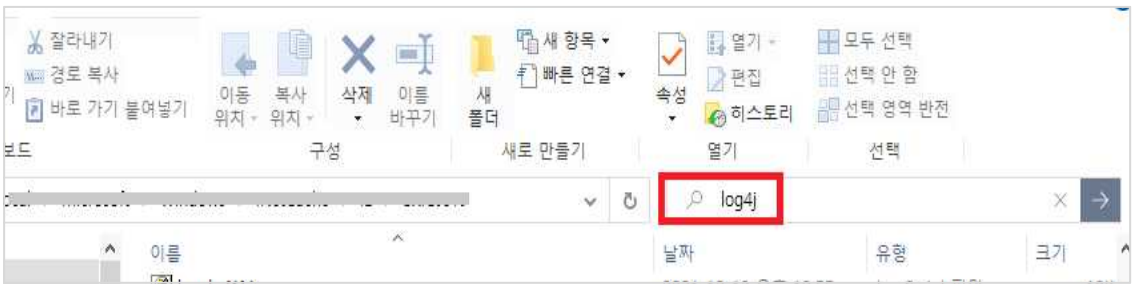
- dpkg –l | grep log4j
- find / -name 'log4j*'



<linux에서 log4j 설치 여부 확인>

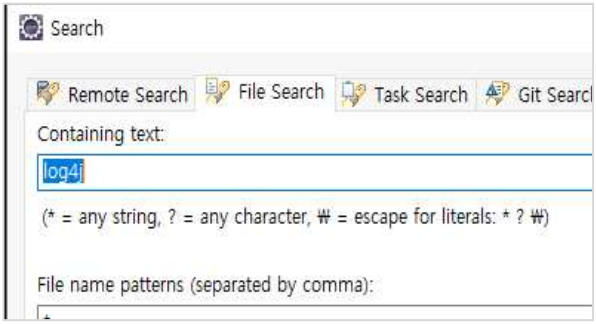
○ log4j 설치 여부 확인(Windows)

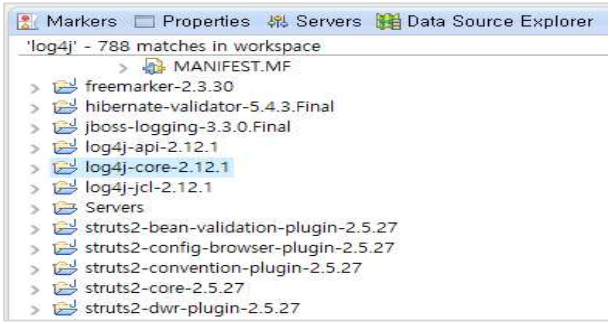
- window explorer의 검색 기능 (log4j 검색)을 이용



<windows explorer의 검색기능을 이용하여 검색>

- (참고) 도구를 활용하는 방법 – eclipse가 설치되어 있는 경우, eclipse의 찾기 기능 활용





<eclipse 도구의 '찾기' 기능을 이용하여 검색>

○ 참고 – 공개되어 있는 도구를 사용하는 방법

- 아래 링크에서 제공하는 도구를 다운로드 한 후 사용법 등을 참고하여 log4j 설치 여부 확인
  * Grype : https://github.com/anchore/grype
  * log4j2-scan : https://github.com/logpresso/CVE-2021-44228-Scanner

Q4. log4j 1.x 버전에서도 영향을 미치나요?

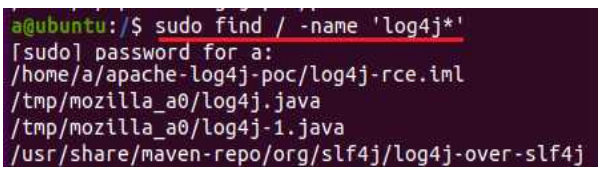
○ log4j 1.x 버전은 CVE-2021-44228, CVE-2021-45046 취약점에는 영향을 받지 않으나, CVE-2021-4104에 해당됩니다.

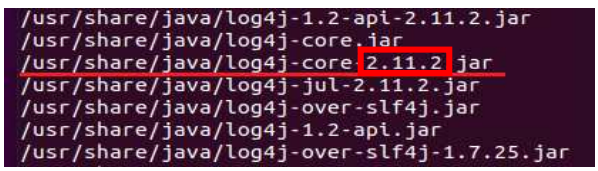
- 본 취약점은 JMSAppender를 사용하지 않는 경우 취약점의 영향은 없으나, 1.x 버전은 이미 2015년 이후 기술지원(업데이트)이 종료되었으므로 보안위협들에 노출될 가능성이 높습니다. 최신버전으로 업데이트 적용하기를 권고합니다.

Q5. 서버 내 설치된 log4j의 버전 확인 방법은 무엇인가요?

○ log4j-core 버전 확인 (linux)

- dpkg –l | grep log4j
- find / -name 'log4j*'

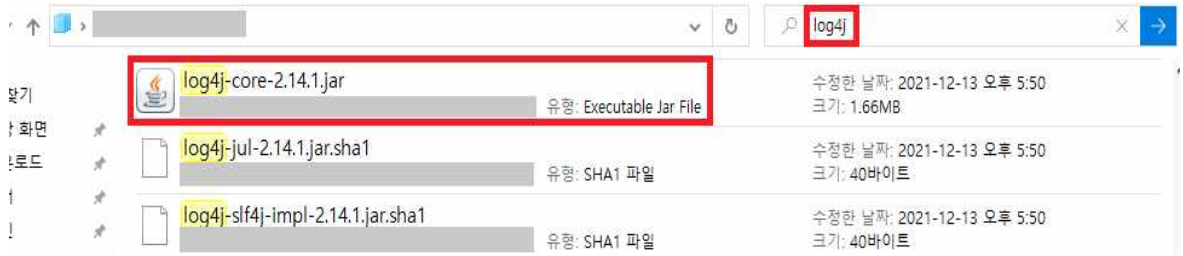




<linux에서 log4j-core 버전 확인>

○ log4j 설치 버전 확인(Windows)

- window explorer의 검색 기능 (log4j 검색)을 이용하여 버전 확인



<Windows 에서 log4j-core 버전 확인>

○ Java Spring Framework Maven 사용 시 log4j가 설치된 경로의 pom.xml 파일을 열어 "**log4j-core**"로 검색

- 검색결과 "<version>사용버전</version>" 으로 확인

```
<!-- https://mvnrepository.com/artifact/org.apache.logging.log4j/log4j-core -->
<dependency>
        <groupId>org.apache.logging.log4j</groupId>
        <artifactId>log4j-core</artifactId>
        <version>2.16.0</version>
</dependency>
```

<log4j-core 버전 정보>

Q6. 버전에 따라 어떻게 조치해야 하나요?
업데이트가 불가능할 경우 어떻게 대응해야 하나요?

○ JAVA사용 버전에 따라 최신 Log4j 버전으로 **업데이트를 수행**하여야 합니다. (Q7 참고)

- JAVA 8 : Log4j 2.16.0 버전으로 업데이트
- JAVA 7 : Log4j 2.12.2 버전으로 업데이트

○ 즉시 업데이트가 어려운 경우 log4j 버전에 따른 해결 방안은 아래와 같습니다.

- CVE-2021-44228, CVE-2021-45046 : **JndiLookup 클래스를 경로에서 제거**
  * zip –q –d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
  ※ log4j-core JAR 파일 없이 log4j-api JAR파일만 사용하는 경우 취약점의 영향을 받지 않음
- CVE-2021-4104 : **JMSAppender 사용 확인 후 코드 수정 또는 삭제**

Q7. 보안 업데이트는 어떻게 하나요?

[주의] 시스템 환경에 따라 다양한 라이브러리가 추가로 적용되어 있을 수 있으므로, 테스트 후 적용을 권고드립니다

※ 현재 시점의 최신버전은 2.16.0이나 log4j 홈페이지를 통해 지속적인 업데이트 확인 필요

○ 최신 파일을 아래의 경로에서 다운로드

- (최신버전 다운로드) https://logging.apache.org/log4j/2.x/download.html

○ 다운로드 한 압축 파일을 해제하고 기존 파일(log4j-core-*.jar)의 경로를 확인하여 log4j-core-*.jar 파일을 해당 경로로 이동

※ 단, 프로그램 호환성 이슈가 있을 수 있으므로, 기존 파일 백업 권고

○ Java Spring Framework Maven을 사용하고 있는 경우 버전 정보 수정 후 재설치, 버전 재확인

① pom.xml을 다음과 같이 수정

```
<dependency>
    <groupId>org.apache.logging.log4j</groupId>
    <artifactId>log4j-core</artifactId>
    <version>2.14.1</version>
</dependency>
```

```
<dependency>
        <groupId>org.apache.logging.log4j</groupId>
        <artifactId>log4j-core</artifactId>
        <version>2.16.0</version
</dependency>
```

<pom.xml 파일 수정>

② mvn install

③ ./mvnw dependency:list | grep log4j or sudo find / -name 'log4j*'로 최신버전 여부 재확인

○ gradle을 사용하고 있는 경우 버전 정보 수정 후 재설치, 버전 재확인

①-1) build.gradle에서 log4j2.version 업데이트

```
ext['log4j2.version'] = '2.16.0'
```

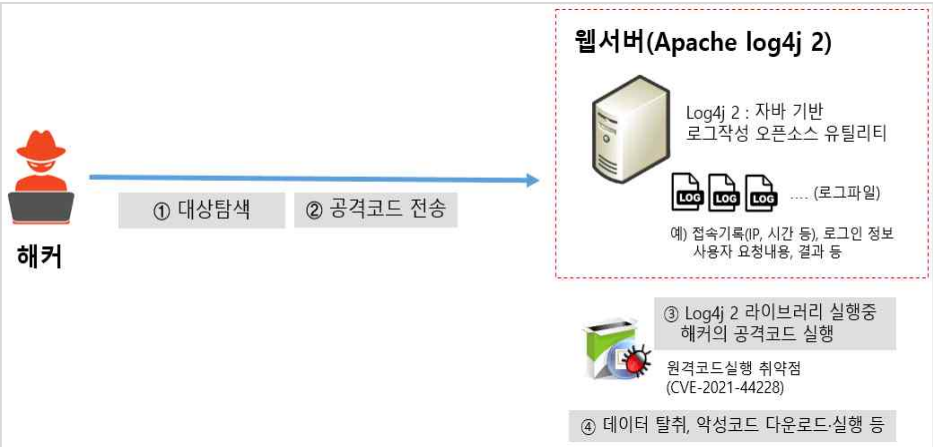
①-2) Gradle 플랫폼 지원을 사용하는 경우

```
implementation(platform("org.apache.logging.log4j:log4j-bom:2.16.0"))
```

② ./gradlew dependencyInsight —dependendy log4j-core로 최신 버전 여부 재확인

Q8. 보안 업데이트를 하지 않으면 어떻게 되나요?

○ 원격의 공격자가 이 취약점을 이용하여 악성코드 유포, 중요 데이터 탈취, 임의의 파일 다운로드 및 실행 등이 가능합니다.



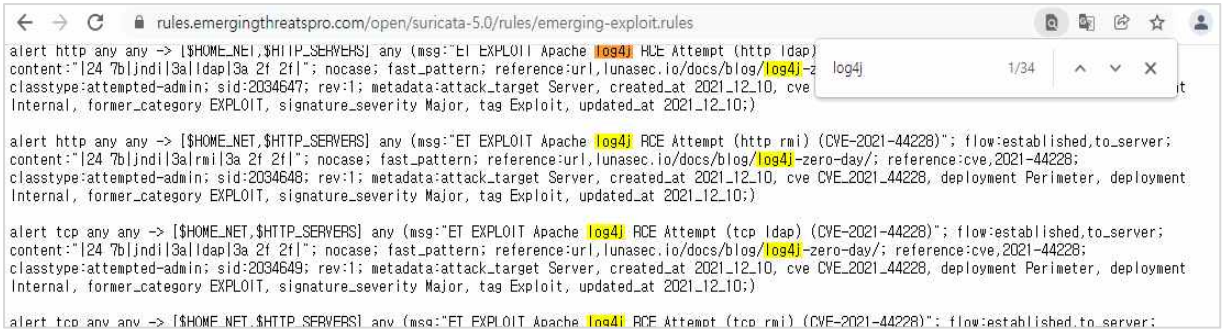
<log4j 취약점 개요도>

Q9. 해당 취약점을 탐지할 수 있는 패턴은 어떻게 작성할 수 있을까요?

○ 아래 링크를 참조하여 log4j로 검색 후 탐지 정책을 확인할 수 있습니다.

- https://rules.emergingthreatspro.com/open/suricata-5.0/rules/emerging-exploit.rules

※ 본 탐지 정책은 내부 시스템 환경에 따라 다르게 동작할 수 있으며 시스템 운영에 영향을 줄 수 있으므로 **충분한 검토 후 적용 바랍니다**. 또한 **우회의 가능성이 있으므로 지속적인 업데이트가 필요함**을 알려드립니다.



Q10. Log4j 취약점을 이용한 침해사고 발생 시 어디에 신고하나요?

○ 아래 침해사고 신고 채널을 통해 신고바랍니다.

- 한국인터넷진흥원 인터넷침해대응센터 종합상황실(02-405-4911 ~ 5, certgen@krcert.or.kr)
- 'KISA 인터넷보호나라&KrCERT' 홈페이지(www.boho.or.kr) → 상담 및 신고 → 해킹 사고

[참고사이트]

○ 보호나라 보안공지 : https://www.boho.or.kr/data/secNoticeView.do?bulletin_writing_sequence=36389
○ Apache 보안업데이트 현황 : https://logging.apache.org/log4j/2.x/security.html
○ CVE-2021-44228 취약점 정보 : https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
○ CVE-2021-45046 취약점 정보 : https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046
○ CVE-2021-4104 취약점 정보 : https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104
○ 최신버전 다운로드 : https://logging.apache.org/log4j/2.x/download.html
○ 제조사별 영향받는 제품 현황 : https://github.com/NCSC-NL/log4shell/tree/main/software
○ 탐지정책 : https://rules.emergingthreatspro.com/open/suricata-5.0/rules/emerging-exploit.rules
○ Log4j 2.12.2버전 다운로드 : https://archive.apache.org/dist/logging/log4j/2.12.2/

본 가이드는 아래 사이트에서 받을 수 있습니다.
[https://www.boho.or.kr/data/guideView.do?bulletin_writing_sequence=36390]