Atlassian, SonarQube 등 Log4j 2 취약점 대처 방안 (Log4JShell)

- **2021-12-17 CVE-2021-45046 및 추가 내용 업데이트**
- **2021-12-20** CVE-2021-45105 내용 업데이트
- 2021-12-21 **ElasticSearch 부분 내용 추가**

이 문서는 Apache Log4j 2에서 발생하는 취약점에 대한 제조사별 대처 방안을 공유하기 위해 작성되었다.

Apache Log4j 2 보안 업데이트 권고

보안 취약 코드

- **CVE-2021-44228**
  - Apache **Log4j 2**에서 발생하는 원격코드 실행 취약점
  - CVE - CVE-2021-44228 (mitre.org)
- **CVE-2021-45046**
  - Apache **Log4j 2**에서 발생하는 서비스 거부 취약점
    (Log4J 기본 구성이 아닌 특정 구성에서 **CVE-2021-44228**를 해결하기 위한 jvm 환경변수 조치사항만으로는 위 보안 이슈에 취약할 수 있음)
  - CVE - CVE-2021-45046 (mitre.org)
- **CVE-2021-4104**
  - Apache **Log4j 1.2**에서 발생하는 원격코드 실행 취약점
  - 1.x 버전의 경우 **JMSAppender**를 사용하지 않는 경우 취약점 영향 없음
- **CVE-2021-45105**
  - Apache **Log4j 2**에서 발생하는 서비스 거부 취약점(CVE-2021-45105)
  - CVE - CVE-2021-45105 (mitre.org)

주요 내용 및 영향 받는 버전, 공통적인 대응방안

KISA 보안공지 - 'Apache Log4j 보안 업데이트 권고' 항목 참고

- https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=36389
- https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=36397 (**CVE-2021-45105**)

추가 참고 URL

- **Apache Log4j 보안 업데이트 현황**
  - Log4j - Apache Log4j Security Vulnerabilities
- **제조사별 현황**
  - log4shell/software at main · NCSC-NL/log4shell · GitHub

제품 별 대처 방안

Atlassian Server & Data Center 제품군

취약여부

- Atlassian 제품군에서는 Atlassian에서 유지 보수하는 **Log4J 1.2.17** 버전을 사용하여 **CVE-2021-44228 / CVE-2021-45046** 보안 이슈에 영향 받지 않으나, Log4J 설정(**log4j.properties**)을 커스터마이징하여 **JMS Appender(org.apache.log4j.JMSAppender)** 기능을 사용할 경우, Bitbucket(Logback 사용)을 제외한 모든 제품에서 **CVE-2021-4104** 보안 이슈에 취약할 수 있음 (보안 심각도: 하)
- 제품별 다음 경로의 **log4.properties(또는 log4j.xml)** 파일을 확인하여 **JMSAppender** 사용여부 확인 필요

Product	Default Path
Jira Server & Data Center	<install-directory>/atlassian-jira/WEB-INF/classes/log4.properties
Confluence Server & Data Center	<install-directory>/confluence/WEB-INF/classes/log4j.properties
Bitbucket Server & Data Center	**Logback 사용하여 영향 없음**
Bamboo Server & Data Center	<install-directory>/atlassian-bamboo/WEB-INF/classes/log4j.properties
Fisheye / Crucible	<install-directory>/log4j.xml
Crowd	<install-directory>/crowd-webapp/WEB-INF/classes/log4j.properties <install-directory>/crowd-openidclient-webapp /WEB-INF/classes/log4j.properties <install-directory>/crowd-openidserver-webapp/WEB-INF/classes/log4j.properties

- **자세한 내용은 아래 Atlassian 공식 문서에서 확인 가능**

조치방안

- **Log4J 설정을 커스터마이징 하지 않았을 경우 아래 Bitbucket ElasticSearch 항목 제외 조치 불필요**
- **Log4J 설정을 커스터마이징하여 JMS Appender을 사용할 경우, log4j.properties** 파일에서 **JMS Appender(org.apache.log4j.JMSAppender)** 관련 라인을 모두 주석 처리 후 솔루션 재기동

공식답변

- FAQ for CVE-2021-44228 and CVE-2021-45046 | Atlassian Support | Atlassian Documentation

Bitbucket Server & Data Center 사용 ElasticSearch

취약여부

- Bitbucket은 Logback을 사용하여 Log4J 2 Shell 이슈에 영향이 없으나, 번들 및 함께 사용하는 ElasticSearch에서 다음의 경우, **CVE-2021-44228/CVE-2021-45046** 보안 이슈에 취약할 수 있음
  - Bitbucket Server를 **JDK8 이하** 버전으로 사용할 경우, 번들로 제공되는 ElasticSearch에서 보안 이슈에 취약할 수 있음
  - BitbucketData Center에서 사용하는 독립적인 ElasticSearch를 **JDK8 이하** 버전으로 사용할 경우, 보안 이슈에 취약할 수 있음
- **아래 ElasticSearch 항목에서 버전별 취약 Matrix 참고**

조치방안

※ Bitbucket Server 기준, 번들로 포함되는 ElasticSearch에 대한 조치 가이드로, DataCenter의 경우 번들이 아닌 독립적인 ElasticSearch 솔루션을 사용하므로, 아래 **ElasticSearch 항목**을 참고하여 조치

1) Bitbucket 버전을 다음 버전으로 업그레이드

- All versions < 6.10.16
- 7.x < 7.6.12
- Versions >= 7.7.0 and < 7.14.2
- 7.15.x < 7.15.3
- 7.16.x < 7.16.3
- 7.17.x < 7.17.4
- 7.18.x < 7.18.3
- 7.19

2) Bitbucket 버전 업그레이드가 불가능할 경우

1. 다음 경로의 **jvm.options(번들 ElasticSearch JVM 설정)** 파일 편집
   Bitbucket Server 기준: <bitbucket-data-directory>/shared/search/**jvm.options**
2. 다음 환경변수 추가 후 저장
   -Dlog4j2.formatMsgNoLookups=true

jvm.options

```
.
.
-Xms4g
-Xmx4g

(  )
## Log4j vulnerability(CVE-2021-44228)
-Dlog4j2.formatMsgNoLookups=true
.
.
```

3. 솔루션 재기동

※ CVE-2021-45046 보안 이슈 대비 JndiLookup.class 삭제

- **5.0.0 ~ 5.6.10, 6.0.0 ~ 6.3.2 버전만 해당, 이외 버전은 위 JVM 환경 변수 추가로 조치됨**
  - 다음 경로에서 ElasticSearch 버전 확인 가능
    - <bitbucket-install-directory>/elasticsearch/lib/**elasticsearch-core-버전.jar**
  - Elastic 공식 가이드
    - https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476

1. Log4J 라이브러리 위치로 이동
   Bitbucket Server 기준: <bitbucket-install-directory>/elasticsearch/lib/**log4j-core-버전.jar**
2. 다음 명령어 수행하여 JndiLookup 클래스 제거 (명령어 수행전 jar파일 백업 필수!)
   $ zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
3. 솔루션 재기동

공식답변

- Multiple Products Security Advisory - Log4j Vulnerable To Remote Code Execution - CVE-2021-44228 | Atlassian Support | Atlassian Documentation

---

SonarSource SonarQube

취약여부

- SonarQube 솔루션은 Log4J의 두가지 인스턴스가 존재하는데, 하나는 SonarQube의 단위 테스트에 사용되지만 외부에서 사용되거나 SonarQube 배포판에 포함되지 않음. 따라서 **CVE-2021-44228** 보안 이슈에 영향 받지 않음
- 다른 하나는 번들로 포함되는 ElasticSearch로, SonarQube를 **JDK8 이하** 버전으로 사용할 경우, **CVE-2021-44228/CVE-2021-45046** 보안 이슈에 취약할 수 있음
  - 공식답변으로 현재 상태에서 위험요소는 없으나, ElasticSearch JVM 환경변수 추가를 통해 보안 조치를 권함
  - 2021-12-16 SonarSouce사는 혼란을 피하기위해 보안 조치가 된 ElasticSearch를 포함하는 SonarQube LTS 버전을 각각 8.9.5 및 9.2.3 버전을 출시함
- **아래 ElasticSearch 항목에서 버전별 취약 Matrix 참고**

조치방안

1) SonarQube 버전을 다음 버전으로 업그레이드

- 8.9.x < 8.9.5
- 9.2.x < 9.2.3

※ LTE 버전만 해당

2) 버전 업그레이드가 불가능할 경우

1. 다음 경로의 sonar.properties(SonarQube 설정) 파일 편집
   <sonarqube-install-directory>/conf/**sonar.properties**
2. **sonar.search.javaAdditionalOpts** 항목 주석 해제 후 다음 환경변수 추가
   sonar.search.javaAdditionalOpts=-Dlog4j2.formatMsgNoLookups=true

   sonar.properties

   ```
   .
   .
   (    )
   ## Log4j vulnerability(CVE-2021-44228)
   sonar.search.javaAdditionalOpts=-Dlog4j2.formatMsgNoLookups=true
   .
   .
   ```

3. 솔루션 재기동

※ CVE-2021-45046 보안 이슈 대비 JndiLookup.class 삭제

- **5.0.0 ~ 5.6.10, 6.0.0 ~ 6.3.2 버전만 해당, 이외 버전은 위 JVM 환경 변수 추가로 조치됨**
  - 다음 경로에서 ElasticSearch 버전 확인 가능
    - <sonarqube-install-directory>/elasticsearch/lib/**elasticsearch-core-버전.jar**
  - Elastic 공식 가이드
    - https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476

1. Log4J 라이브러리 위치로 이동
   <sonarqube-install-directory>/elasticsearch/lib/**log4j-core-버전.jar**
2. 다음 명령어 수행하여 JndiLookup 클래스 제거 (명령어 수행전 jar파일 백업 필수!)
   $ zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
3. 솔루션 재기동

공식답변

- SonarQube, SonarCloud, and the Log4J vulnerability - SonarSource Updates / Announcements - SonarSource Community

---

Jfrog Artifactory

취약여부

- JFrog Security 팀 내부 조사 및 검증 결과 JFrog 제품들은 위 보안 이슈에 영향받지 않음

조치방안

- **조치 불필요**

공식답변

- https://twitter.com/jfrog/status/1469385793823199240

Sonatype Nexus

취약여부

- Sonatype 솔루션은 Log4J 대신 **Logback**을 사용하여 위 보안 이슈에 영향받지 않음

조치방안

- **조치 불필요**

공식답변

- https://blog.sonatype.com/a-new-0-day-log4j-vulnerability-discovered-in-the-wild

---

Elastic ElasticSearch

※ Bitbucket DataCetner 사용시 번들이 아닌 독립적으로 설치하여 사용하기 때문에 해당 항목 기재함

취약여부

- JDK(jdk9+)의 최근 버전과 함께 사용되는 ElasticSearch 6(6.8.9+) 및 7(7.8+) 버전은 Java Security Manager를 사용하기 때문에 CVE-2021-44228 보안 이슈의 원격 코드 실행에 취약하지 않음
- 대부분의 다른 버전(5.6.11+, 6.4.9+, 7.0.0+)은 CVE-2021-44228 보안 이슈에 취약할 수 있음
- 14일에 발표된 추가 취약점(CVE-2021-45046)에는 영향 받지 않음

※ Elasticsearch mitigation summary Matrix

Elasticsearch	JDK	CVE IDs	Information Leak	Remote Code Execution	Complete Mitigation
7.16.1 - 7.16.2	≥ 8	CVE-2021-44228, CVE-2021-45046	No	No	N/A (not vulnerable)
7.0.0 - 7.16.0	≥ 9	CVE-2021-44228, CVE-2021-45046	No	No	N/A[3] (not vulnerable)
7.0.0 - 7.16.0	< 9	CVE-2021-44228, CVE-2021-45046	Yes	No	System property[1]
6.8.21	≥ 8	CVE-2021-44228, CVE-2021-45046	No	No	N/A (not vulnerable)
6.0.0 - 6.8.20	≥ 9	CVE-2021-44228, CVE-2021-45046	No	No	N/A[3] (not vulnerable)
6.4.0 - 6.8.20	< 9	CVE-2021-44228, CVE-2021-45046	Yes	No	System property[1]
6.0.0 - 6.3.2	< 9	CVE-2021-44228, CVE-2021-45046	Yes	No	Remove JndiLookup[2]
5.6.11 - 5.6.16	8	CVE-2021-44228, CVE-2021-45046	Yes	Yes	System property[1]
5.0.0 - 5.6.10	8	CVE-2021-44228, CVE-2021-45046	Yes	Yes	Remove JndiLookup[2]
< 5.0.0	any	CVE-2021-44228, CVE-2021-45046	No	No	N/A (not vulnerable)

출저: Elastic 공식답변 URL

조치방안

1) ElasticSearch 버전을 다음 버전으로 업그레이드

- 6.8.22 or 7.16.2

2) 버전 업그레이드가 불가능할 경우

1. 다음 경로의 **jvm.options(ElasticSearch JVM 설정)** 파일 편집
   tar 또는 zip 배포판: <elasticsearch-directory>/config/**jvm.options**
   RPM 패키지 설치시: /etc/elasticsearch/**jvm.options**

2. 다음 환경변수 추가 후 저장
   -Dlog4j2.formatMsgNoLookups=true

   jvm.options

   ```
   .
   .
   (  )
   ## Log4j vulnerability(CVE-2021-44228)
   -Dlog4j2.formatMsgNoLookups=true
   .
   .
   ```

3. 솔루션 재기동

※ CVE-2021-45046 보안 이슈 대비 JndiLookup.class 삭제

- **5.0.0 ~ 5.6.10, 6.0.0 ~ 6.3.2 버전만 해당, 이외 버전은 위 JVM 환경 변수 추가로 조치됨**
  - Elastic 공식 가이드
    - https://discuss.elastic.co/t/apache-log4j2-remote-code-execution-rce-vulnerability-cve-2021-44228-esa-2021-31/291476

1. Log4J 라이브러리 위치로 이동
   tar 또는 zip 배포판: <elasticsearch-directory>/lib/**log4j-core-버전.jar**
   RPM 패키지 설치시: /etc/elasticsearch/lib/**log4j-core-버전.jar**

2. 다음 명령어 수행하여 JndiLookup 클래스 제거 (명령어 수행전 jar파일 백업 필수!)
   $ zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class

3. 솔루션 재기동

공식답변

- Apache Log4j2 Remote Code Execution (RCE) Vulnerability - CVE-2021-44228 - ESA-2021-31 - Announcements / Security Announcements - Discuss the Elastic Stack