

EPP 서버 log4j 2.x 취약점 조치 가이드

경기도 성남시 분당구 판교역로 220 (우) 13493 | 대표전화 : 031-722-8000 | 팩스 : 031-722-8901 | www.ahnlab.com
© AhnLab, Inc. All rights reserved.

1. 개요

본 문서는 EPP 서버에 대한 log4j 2.x 취약점 수동 조치 방법을 기술합니다.

2. 조치 방법

1) 스크립트 업로드

- 스크립트 파일: log4j_patch.sh
- WinSCP, Filezilla 등의 툴을 사용해 EPP 서버의 임의 경로에 log4j_patch.sh 업로드 합니다.

2) 스크립트 실행

- ① ssh로 접속하여 root 권한을 획득하고 1)에서 업로드한 경로로 이동합니다.
- ② 스크립트에 실행 권한을 부여합니다.


```
# chmod +x ./log4j_patch.sh
```
- ③ 스크립트를 실행합니다.


```
# ./log4j_patch.sh
```
- ④ 실행 결과를 확인합니다.
 - 스크립트 실행이 완료되면 아래 화면이 출력됩니다.
 - 가운데 점선을 기준으로 위에는 실행 전 log4j 관련 파일들이, 아래에는 실행 후 log4j 관련 파일들이 나열됩니다.
 - 실행 전과 후의 파일 소유권이 같아야 합니다.
 - 실행 후 파일 크기가 작아져야 합니다.

(예시 화면)

```
[root@ep epp a log4j_script]# ./log4j_patch.sh
7879677 1376 -r-xr----- 1 eppcli epp 1407853 12월 18 2018 /opt/ahnlab/epp/lib/java/log4j-core-2.8.2.jar
1610948452 1376 -r-xr----- 1 eppcli epp 1407853 12월 18 2018 /opt/ahnlab/epp/service/tomcat-auth/webcontext/WEB-INF/lib/log4j-core-2.8.2.jar
1074917295 1376 -r-xr----- 1 eppcli epp 1407853 12월 18 2018 /opt/ahnlab/epp/service/tomcat-console/webcontext/WEB-INF/lib/log4j-core-2.8.2.jar
837348159 1376 -r-xr----- 1 eppcli epp 1407853 12월 18 2018 /opt/ahnlab/epp/service/tomcat-agent/webcontext/WEB-INF/lib/log4j-core-2.8.2.jar
837348071 1376 -r-xr----- 1 eppcli epp 1407853 12월 18 2018 /opt/ahnlab/epp/service/batch-processor/libs/log4j-core-2.8.2.jar
837348426 1376 -r-xr----- 1 eppcli epp 1407853 12월 18 2018 /opt/ahnlab/epp/service/cluster-manager/libs/log4j-core-2.8.2.jar
8687233 1376 -r-xr----- 1 eppcli epp 1407853 12월 18 2018 /opt/ahnlab/epp/service/report-processor/libs/log4j-core-2.8.2.jar
1610894004 1376 -r-xr----- 1 eppcli epp 1407853 12월 18 2018 /opt/ahnlab/epp/service/kafka-consumer/libs/log4j-core-2.8.2.jar
837323794 1376 -r-xr----- 1 eppcli epp 1407853 12월 18 2018 /opt/ahnlab/epp/service/scheduler/libs/log4j-core-2.8.2.jar
-----
487360 1360 -r-xr----- 1 eppcli epp 1391325 12월 13 09:16 /opt/ahnlab/epp/lib/java/log4j-core-2.8.2.jar
1610893573 1360 -r-xr----- 1 eppcli epp 1391325 12월 13 09:16 /opt/ahnlab/epp/service/tomcat-auth/webcontext/WEB-INF/lib/log4j-core-2.8.2.jar
1074821559 1360 -r-xr----- 1 eppcli epp 1391325 12월 13 09:16 /opt/ahnlab/epp/service/tomcat-console/webcontext/WEB-INF/lib/log4j-core-2.8.2.jar
837504047 1360 -r-xr----- 1 eppcli epp 1391325 12월 13 09:16 /opt/ahnlab/epp/service/tomcat-agent/webcontext/WEB-INF/lib/log4j-core-2.8.2.jar
837331185 1360 -r-xr----- 1 eppcli epp 1391325 12월 13 09:16 /opt/ahnlab/epp/service/batch-processor/libs/log4j-core-2.8.2.jar
837038674 1360 -r-xr----- 1 eppcli epp 1391325 12월 13 09:16 /opt/ahnlab/epp/service/cluster-manager/libs/log4j-core-2.8.2.jar
487377 1360 -r-xr----- 1 eppcli epp 1391325 12월 13 09:16 /opt/ahnlab/epp/service/report-processor/libs/log4j-core-2.8.2.jar
1610948452 1360 -r-xr----- 1 eppcli epp 1391325 12월 13 09:16 /opt/ahnlab/epp/service/kafka-consumer/libs/log4j-core-2.8.2.jar
837508500 1360 -r-xr----- 1 eppcli epp 1391325 12월 13 09:16 /opt/ahnlab/epp/service/scheduler/libs/log4j-core-2.8.2.jar
```

※ 소유권이 변경되었을 경우

- eppuser 확인


```
# stat -c '%U' /opt/ahnlab/epp
```
- 확인된 eppuser(ex. eppcli)를 이용해 소유권 변경


```
# find /opt/ahnlab/epp -name log4j-core*.jar -exec chown eppcli:epp {} \;
```
- 정상적으로 변경이 되었는지 확인


```
# find /opt/ahnlab/epp -name log4j-core*.jar -ls
```

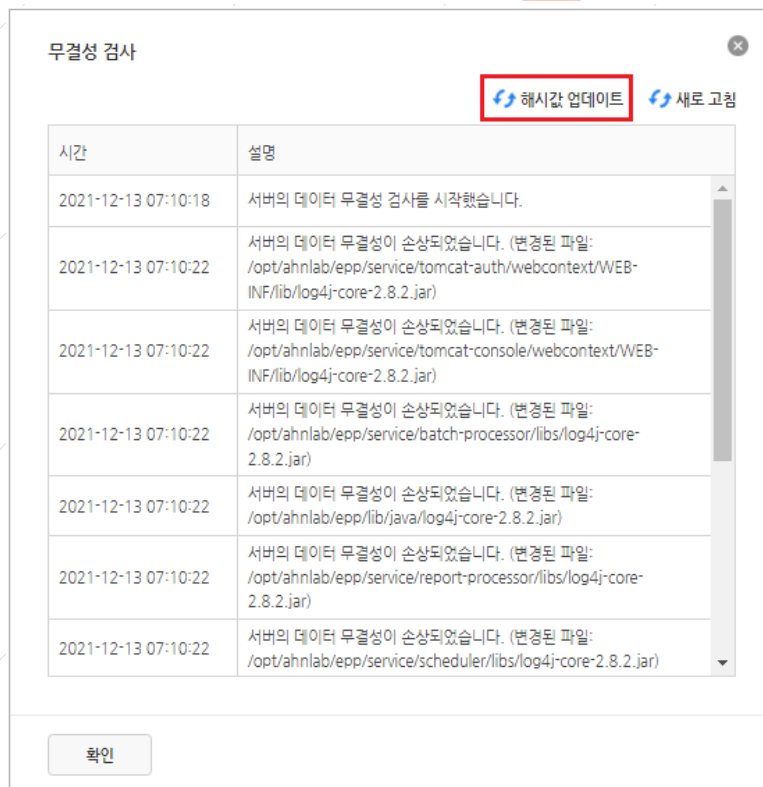
3) 서비스 재시작

```
[root@localhost ~]# stopmgr
```

[root@localhost ~]# startmgr

4) 해시값 업데이트

- ① 정상적으로 수행이 되었다면 jar 파일 변경으로 무결성이 깨지게 되어 도메인 현황에 붉은색으로 무결성 손상에 표시가 됩니다. (붉은색 표시가 되었는지 확인 필요)
- ② 웹 콘솔 로그인 > 대시보드 > 도메인 현황> 무결성 검사 내역 보기 > 해시값 업데이트



- ③ 잠시 후 무결성 손상이 초록색 불로 바뀌었는지 확인