- description : 톰캣 보안패치 (Tomcat)
- author : 김토피아
- email : kimmk@repia.com
- lastupdate : 2023-07-06

취약점 내용

항목명 : 로그 포맷 설정
중요도 : 상
항목개요 : 로그 포맷을 설정하지 않으면, 공격 여부 파악, 공격자 사용 툴 파악, 공격자 위치 파악이 불가능하므로 반드시 로그 포맷을 설정해야 함

판단기준

양호: 로그 포맷 설정 값이 combined 이거나 그에 준하는 포맷 스트링으로 설정되어 있는 경우
취약: 로그 포맷 설정 값이 combined 가 아니거나 그에 준하지 않는 포맷 스트링으로 설정되어 있는 경우

처리방법

1. server.xml 파일 수정

```
shell> cd /usr/local/tomcat/conf
shell> vi server.xml
shell> ls -al
-rw-r----- 1 search search 8153  7월 6 14:34 catalina.out
```

2. tomcat 설정 변경

```
shell> cd /usr/local/tomcat/bin/
shell> vi catalina.sh

pattern 속성의 기존 내용 또는 비어 있는 내용이 있으면 아래와 같이 combined로 변경 후 저장하고 Tomcat을 재시작 한다.

       <!-- Access log processes all example.
            Documentation at: /docs/config/valve.html
            Note: The pattern used is equivalent to using pattern="common"
-->
        <Valve className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
               prefix="localhost_access_log" suffix=".txt"
               pattern="combined" />
```

```
로그 출력 내용 변경 됨 ( localhost_access_log.2023-07-06.txt )
변경 전 : 125.132.25.161 - - [05/Sep/2022:17:55:42 +0900] "GET
/search/front_best/search.jsp HTTP/1.1" 200 2123
변경 후 : 125.132.25.161 - - [05/Jul/2023:16:08:57 +0900] "GET /index.jsp
HTTP/1.1" 200 13 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36
Edg/114.0.1823.58"
```

Ref

김토피아, 취약점

From:
http://125.132.25.164/dokuwiki/ - **문제를 잘 정의하는 것은 문제를 절반 해결한 것이다. - 2023.12**

Permanent link:
http://125.132.25.164/dokuwiki/doku.php?id=was:tomcat:%EB%A1%9C%EA%B7%B8_%ED%8F%AC%EB%A7%B7_%EC%84%A4%EC%A0%95&rev=1688625657

Last update: **2023/07/06 15:40**