OC (상)	운영체제 명령 실행
취약점 개요	
점검목적	■ 적절한 검증절차를 거치지 않은 사용자 입력 값에 의해 의도하지 않은 시스템 명령어가 실행되는 것을 방지하기 위함
보안위협	■ 해당 취약점이 존재하는 경우 부적절하게 권한이 변경되거나 시스템 동작 및 운영에 악영향을 줄 가능성이 있으므로 "|", "&", ";", "`" 문자에 대한 필터링 구현이 필요함
참고	CVE/NVD - 공개적으로 알려진 취약점 검색 가능 http://cve.mitre.org/cve/search_cve_list.html https://nvd.nist.gov/vuln/search ※ 사용 중인 웹 서버 버전 확인, 소스코드 및 취약점 점검 필요
조치방법	취약한 버전의 웹 서버 및 웹 애플리케이션 서버는 최신 버전으로 업데이트를 적용해야 하며, 애플리케이션은 운영체제로부터 명령어를 직접적으로 호출하지 않도록 구현하는 게 좋지만, 부득이하게 사용해야 할 경우 소스 코드나 웹 방화벽에서 특수문자, 특수 구문에 대한 검증을 할 수 있도록 조치해야 함

보안설정 방법

웹 방화벽에 모든 사용자 입력 값을 대상으로 악용될 수 있는 특수문자, 특수 구문 등을 필터링 할 수 있도록 규칙 적용

* 애플리케이션은 운영체제로부터 명령어를 직접적으로 호출하지 않도록 구현
* 명령어를 직접 호출하는 것이 필요한 경우에는, 데이터가 OS의 명령어 해석기에 전달되기 전에 입력 값을 검증/확인하도록 구현
* 입력 값에 대한 파라미터 데이터의 "&", "|", ";", "`" 문자에 대한 필터링 처리

※ 참고: "&", "|", "`" 문자 설명
- & : 윈도우 명령어 해석기에서 첫 번째 명령이 성공했을 경우만 두 번째 명령어를 실행
- | : 첫 번째 명령어가 성공하는지에 상관없이 두 번째 명령어를 실행
- ` : 쉘 해석기가 명령어를 해석하다 역 작은따옴표(`) 내에 포함된 명령어를 만나면 기존 명령어를 계속 실행하기 전에 역 작은따옴표로 둘러싸인 명령어를 먼저 실행
  (예) `ls –al`

* 웹 서버 및 웹 애플리케이션 서버는 공개적으로 알려진 취약점이 제거된 상위 버전으로 업데이트해야 함

※ KISA 인터넷 보호나&KrCERT 보안공지 참고
https://www.boho.or.kr/data/secNoticeList.do

* 클라이언트에서 전송되는 요청(Request) 값에 대한 엄격한 필터링 적용 및 OGNL (Object Graph Navigation Language) 표현식 사용을 금지하여 원격에서 임의의 명령어가 실행되지 않도록 구현해야 함