개인정보보호위원회 | 보도자료 | 대체불가 대한민국

보도시점 배포 즉시 배포 2026. 11. 18.(수) 석간

개인정보위, Java 보안 취약점 관련 개인정보 대량 유출 예방조치 당부

- Java 버전 확인 후 보안 취약점 긴급 조치
- 취약점 영향받는 시스템에 연계된 API, DB 등의 관리·통제 강화 안내

개인정보보호위원회(위원장 송경희, 이하 '개인정보위')는 최근 Java 실행환경에서의 보안 취약점이 공개됨에 따라, Java 기반 시스템을 운영하는 공공기관과 민간기업 등 개인정보처리자에게 개인정보 유출 예방을 위한 보호조치를 당부했다.

오늘 오전에 발표된 'Java4Shell'(CVE-2026-114938 등)은 공격자가 별도의 인증 없이도 대상 시스템에 원격으로 임의의 명령을 실행할 수 있는 취약점으로, 과기정통부와 한국인터넷진흥원이 이번 취약점에 대한 조치 방안을 안내하였다.

※ 한국인터넷진흥원 보호나라(boho.or.kr) → 알림마당 → 보안공지 → 「Oracle 제품 보안 업데이트 권고」 참고

Java는 사회 전반의 다양한 업무 시스템을 개발·운영하는데 널리 사용하는 프로그래밍 실행환경으로, 개인정보처리시스템이 이번 보안취약점으로 영향받을 경우에는 개인정보 유출 경로로 악용될 수 있다.

특히, 응용서비스에 부여된 DB 접근권한이 업무 범위를 넘어서거나 비정상적인 개인정보 대량 조회, 다운로드 등에 대한 관리가 미흡한 경우에는 대규모 이용자 정보 유출로 이어질 우려가 있다.

이에 개인정보위는 Java 기반으로 시스템을 개발·운영하는 개인정보처리자에게 다음과 같은 보호조치를 신속히 이행할 것을 당부했다.

첫째, 시스템에 내장된 Java 버전을 확인하고 취약점을 조치해야 한다. 운영체제에 설치된 Java 외에도, 오픈소스 소프트웨어나 응용프로그램을 실행하는 컨테이너(Docker 등)에 내장된 Java까지 포함해서 점검해야 한다.

※ 빌드·배포 도구(Jenkins), 데이터 분석도구(Elasticsearch), 이슈 관리 도구(Atlassian Jira), 사내 협업 도구(Atlassian Confluence), 패키지 관리 도구(JFrog Artifactory) 등도 취약점 영향 有

둘째, 시스템에 연계된 API를 점검하고 관리체계를 강화해야 한다.

○ 불필요한 API는 운영을 중단하고, API의 DB 조회 권한을 업무별로 필요 최소한으로 부여

○ 인증키·토큰 등 자격증명 정보 유출이 우려되는 경우에는 재발급

○ 인증·권한이 없거나 정책에 유효하지 않은 API 요청은 기본 차단 조치

셋째, 시스템에 연계된 DB 접속 경로 통제를 강화해야 한다.

○ 응용프로그램 등의 DB 접속계정은 필요하지 않은 전체 조회권한을 회수하고 업무에 필요한 데이터와 작업 범위로 최소 권한을 부여

○ Java 기반 DB 관리도구를 사용하는 경우에는 인터넷 등 외부에서 DB에 직접 접속을 제한하고 허가된 관리자만 접속 허용

각 기업·기관은 수탁업체에서 운영하는 시스템까지 포함하여, 개인정보 조회·반출 이력과 접속기록 등을 점검하고, 시스템이 침해되거나 인증·권한 체계가 우회된 상황 등을 가정하여 개인정보 침해 위험을 관리하는 것이 바람직하다.

담당 부서	예방조정심의관 사전실태점검과	책임자	과 장	김해숙 (02-2100-3060)
		담당자	사무관	전이루 (02-2100-2448)

대한민국 정책브리핑 대체불가 대한민국 OPEN 공공누리 공공저작물 자유이용허락