과학기술정보통신부 보도자료 대체불가 대한민국

보도 시점 배포 시점 배포 2026. 11. 18.(수) 07시

과기정통부, 자바(Java) 보안 취약점 관련 긴급 점검 및 보안조치 당부

- 자바 버전과 실행환경 확인...인터넷에 공개된 서비스부터 우선 조치 -

- 취약점 수정 업데이트 제공 시 신속 적용, 적용 후 재시작 및 반영 여부 확인 -

과학기술정보통신부(부총리 겸 과학기술정보통신부 장관 배경훈, 이하 '과기정통부')와 한국인터넷진흥원(이하 'KISA')은 자바(Java) 실행환경인 오픈제이디케이(OpenJDK)에서 **보안 취약점이 발견**됨에 따라, **긴급 점검과 보안 업데이트를 권고**하였다. 관련 취약점을 공격자가 악용할 경우 악성코드 실행 등의 피해가 발생할 수 있으므로, 아래 보호나라 보안공지에 따라 **신속하게 보안조치를 해줄 것을 당부**하였다.

※ 한국인터넷진흥원(KISA) 보호나라(www.boho.or.kr) 알림 마당 → 보안공지

자바(Java)란 **웹서비스, 그룹웨어, ERP 등 다양한 프로그램을 개발하고 실행**하는데 사용하는 **기반 프로그램**으로, 기업이 직접 설치하거나 다른 소프트웨어·장비에 포함되어 사용된다. **이번 취약점**(Java4Shell, CVE-2026-114938 등)은 비정상적인 입력을 처리하는 과정에서 메모리 손상이 생기는 문제로, 일부 프로그램에서는 **공격자가 인증 없이 원격에서 임의의 코드를 실행**할 수 있어 주의가 필요하다.

이번 취약점은 Oracle Java SE 17.0.21.0.3을 비롯한 일부 Java 및 GraalVM 제품에 영향을 미치므로, 기업과 기관은 사용중인 제품의 버전과 실행환경을 확인하고 제조사가 안내한 보안조치를 신속히 이행해야 한다.

이에 기업·기관은 **인터넷에 공개된 서비스, 그룹웨어, ERP, 핵심 업무 시스템부터 우선 점검**하고, 보안공지에서 제공하는 **보안 업데이트를 신속하게 적용**해야 한다. 업데이트 후에는 실제 운영중인 서비스에 **반영되었는지 반드시 확인**해야 한다.

과기정통부와 KISA는 **보호나라 홈페이지에 보안공지를 게시**하고, 주요정보통신기반시설, 정보보호관리체계(ISMS) 인증기업, 정보보호최고책임자(CISO) 신고기업 등 주요 기업에 신속한 조치를 안내했다.

※ 통신·ISP, 보안관제·백신, 호스팅, 협회·단체, 방산, 조선 등

관련 **보안 취약점 조치에 대한 자세한 사항**은 보호나라 홈페이지 **보안공지를 참고**하고, 국번없이 **118로 연락하면 상담 및 지원**을 받을 수 있다.

담당 부서	정보보호네트워크정책관 사이버침해대응과	책임자
		담당자
유관 기관	한국인터넷진흥원 디지털위협대응본부	책임자
		담당자

대체불가 대한민국 내실을 만드는 과학기술 내삶을 채우는 디지털·AI 대한민국 정책브리핑