오픈소스 공급망 공격 사례 분석

메인테이너 계정 탈취에서 배포까지 6시간

요 약

널리 사용되는 오픈소스 패키지의 메인테이너 계정이 탈취되어 악성 코드가 삽입된 버전이 배포된 사건을 분석했다. 악성 코드는 설치 스크립트 단계에서 실행되어 환경변수와 CI 토큰을 외부로 전송했으며, 게시부터 탐지까지 약 6시간 동안 수만 건이 내려받아졌다.

1. 사건 경과

메인테이너의 인증 정보가 별도 유출 사고에서 확보된 자격 증명 재사용으로 탈취된 것으로 추정된다. 2단계 인증이 적용되지 않은 계정이었다.

2. 악성 코드 동작

패키지 설치 시 자동 실행되는 스크립트에서 환경변수 전체를 수집해 외부 엔드포인트로 전송했다. CI 환경에서 실행될 경우 배포 자격 증명까지 노출된다.

3. 방어 전략

의존성 버전 고정과 해시 검증, CI에서의 설치 스크립트 비활성화, 사내 프록시 레지스트리를 통한 신규 버전 격리 기간 설정이 효과적이다.

4. 대응 성숙도

우리 서비스에 특정 패키지가 포함되어 있는지 30분 안에 답할 수 있는가가 실질적인 성숙도 지표다. SBOM 확보를 우선 과제로 제안한다.