

우리 일상이 된 쇼핑 앱은 왜 뚫렸나? JWT 인증의 명과 암

2025년말, 국내 최대 이커머스 플랫폼 개인정보 유출 사태가 불거졌다. 2025년 12월 기준, 유출 규모는 3천만 건이 넘는 것으로 알려졌다. 이번 보안 사고의 핵심은 해당 기업의 JWT(JSON Web Token) 인증 시스템이 취약하게 관리되었다는 점이다. 당사에서 근무했던 개발자의 JWT 서명키가 퇴사 후에도 리셋되지 않았고, 공격자는 유효한 서명키를 활용해 고객 정보를 제한 없이 조회할 수 있었다.

이번 사건의 중심에 있는 JWT 인증은 현대 웹/모바일 애플리케이션의 표준으로 자리잡고 있다. 무상태(stateless) 인증의 편리함을 제공하지만, 관리가 제대로 되지 않으면 인증 체계 전체를 붕괴시킬 수 있는 단일 실패 지점(Single Point of Failure)이 될 수도 있다.

이번 보고서에서는 JWT의 개념과 인증 방식을 소개한 뒤, CVE 사례 중심으로 주요 취약점을 분석하고 이를 예방 및 완화하기 위한 실질적인 보안 전략을 제시한다.

▶ 보고서 다운로드

AhnLab

A-FIRST팀 조한준 매니저