클라우드 스토리지 설정 오류로 인한 데이터 노출

취약점보다 흔하고, 패치도 없다

요 약

오브젝트 스토리지 버킷이 퍼블릭으로 공개되어 회원 문서가 노출된 사례를 분석했다. 원인은 개발 단계에서 임시로 부여한 권한이 그대로 운영 환경에 반영된 것으로, 코드 취약점이 아닌 설정 오류에 해당한다. 이러한 유형은 벤더가 제공하는 패치가 존재하지 않으므로 조직의 통제 절차로만 예방할 수 있다.

1. 노출 경위

개발 편의를 위해 부여한 퍼블릭 읽기 권한이 운영 배포 시 함께 반영됐다. 내부 점검에서는 인증된 세션으로만 확인해 문제를 발견하지 못했다.

2. 점검 방법

계정 단위의 퍼블릭 액세스 차단을 강제하고, IaC 코드에 정책 검사를 붙인다. 정기적으로 외부 관점에서 스캔해야 하며, 내부에서만 보면 찾을 수 없다.

3. 사후 조치

접근 로그를 확보해 실제 다운로드 여부와 범위를 산정하고, 영향받은 이용자에게 통지한다. 로그 보존 기간이 짧으면 범위 산정 자체가 불가능해진다.

4. 재발 방지

권한 변경을 코드 리뷰 대상에 포함하고, 배포 파이프라인에 정책 위반 차단 게이트를 둔다.