# VPN 장비 인증 우회 취약점 긴급 권고

CVSS 9.8 · 즉시 조치 필요

요 약

주요 VPN 게이트웨이 제품군에서 인증을 우회해 관리자 권한을 획득할 수 있는 취약점이 확인됐다. 인터넷에 관리 인터페이스가 노출된 환경에서는 사전 인증 없이 원격 코드 실행으로 이어질 수 있어 즉시 조치가 필요하다. PoC 공개까지의 시간이 짧을 것으로 예상되므로 패치 배포를 기다리기보다 노출 차단을 우선할 것을 권고한다.

## 1. 영향 범위

영향을 받는 버전과 구성은 벤더 권고문을 참고한다. 관리 인터페이스가 외부에서 접근 가능한 모든 장비가 대상이며, 내부망 전용 구성이라도 측면 이동 경로가 있는 경우 위험도가 낮아지지 않는다.

## 2. 임시 완화책

관리 인터페이스의 외부 접근을 즉시 차단하고 접속 IP 화이트리스트를 적용한다. 관리자 계정에 MFA를 강제하고, 발급된 세션 토큰을 전량 무효화한 뒤 재로그인을 요구한다.

## 3. 침해 여부 조사

패치는 재발 방지 수단이지 사고 종결이 아니다. 취약점 공개 시점 이전으로 소급해 비정상 인증 성공, 신규 관리자 계정 생성, 설정 변경 이력을 조사해야 한다.

## 4. 탐지 지표

인증 로그에서 동일 세션 식별자의 반복 사용, 비업무 시간대의 관리자 로그인, 지리적으로 불일치하는 접속 원본을 우선 확인한다.