GN-SA-2026-003: Genian NAC - CWP User Search: Unauthenticated Administrator Credential Disclosure Vulnerability

날짜

- 2026년 07월 22일

CVE ID

- CVE-2026-16520

CVSS V4.0 score

- 8.7

영향도

- 높음

내용

Genian NAC 미인증 상태에서 CWP 사용자 검색기를 이용한 관리자 자격 증명 획득 취약점이 발견되어 조치와 함께 제품 보안성 강화를 위한 보안 업데이트를 발표했습니다. 영향 버전을 사용하는 이용자들은 최신 버전으로 업데이트를 권고합니다.

영향 버전

- Genian NAC 4.0.175 Release (Revision 150340 미만)
- Genian NAC 5.0.65 LTS Release (Revision 150331 미만)

- Genian NAC 5.0.75 LTS Release (Revision 150330 미만)
- Genian NAC 5.0.87 Release Stable (Revision 150329 미만)
- Genian NAC 5.0.88 Release (Revision 150328 미만)
- Genian ZTNA 6.0.26 LTS Release (Revision 150337 미만)
- Genian ZTNA 6.0.35 LTS Release (Revision 150336 미만)
- Genian ZTNA 6.0.47 Release Stable (Revision 150334 미만)
- Genian ZTNA 6.0.48 Release (Revision 150333 미만)

해결 방법

이 권고 사항에 포함된 취약점은 아래 버전으로 업데이트하여 해결할 수 있습니다.

- Genian NAC 4.0.175 Release (Revision 150340 이상)
- Genian NAC 5.0.65 LTS Release (Revision 150331 이상)
- Genian NAC 5.0.75 LTS Release (Revision 150330 이상)
- Genian NAC 5.0.87 Release Stable (Revision 150329 이상)
- Genian NAC 5.0.88 Release (Revision 150328 이상)
- Genian ZTNA 6.0.26 LTS Release (Revision 150337 이상)
- Genian ZTNA 6.0.35 LTS Release (Revision 150336 이상)
- Genian ZTNA 6.0.47 Release Stable (Revision 150334 이상)
- Genian ZTNA 6.0.48 Release (Revision 150333 이상)

임시 조치 방법

- 사용자 검색기 기능을 사용하지 않는 환경에서는 해당 기능에 대한 접근을 차단하여 임시 조치할 수 있습니다. 상세 방법은 제조사 기술지원센터(TAC) 또는 전문 기술지원업체를 통해 안내받을 수 있습니다.