# 휴네시온 시스템접근제어 NGS 제품 보안 취약점 조치계획 안내

2023.12.21.

휴네시온 시스템 접근제어 NGS 제품의 보안 취약점 발생에 따라 취약점 관련 내용 및 조치 계획에 대하여 안내 드리며, 조속한 상황 해결을 위해 최선의 노력을 기울일 것을 약속 드립니다.

가. 제품 정보

o 제품명: NGS V6.0, NGS V7.0, i-oneNGS V2.0

나. 보안 취약점 내용 및 영향 버전

| No. | 취약점 내용 | 영향 버전 |
|---|---|---|
| 1 | 로그인 없이 관리자 ID 확인 및 타인 비밀번호 무단 변경 가능한 URL 노출 및 접근 가능 | V6.0, V7.0 |
| 2 | URL 변경을 통해 관리자용 사용자권한 수정 페이지에 무단 접속하여 관리자 권한으로 권한상승 가능 | V6.0, V7.0 |
| 3 | 장비의 시스템 계정 패스워드가 평문으로 노출됨 | V6.0, V7.0, i-oneNGS V2.0 |
| 4 | 파일 다움로드 취약점으로 인해 DB 접속 정보 노출 | V6.0, V7.0, i-oneNGS V2.0 |

다. 보안 취약점 조치 진행 계획

1) 보안취약점에 항목에 대하여 **2023.12.28.까지 패치버전 준비 완료**

2) 기술지원본부에서 고객별 일정 협의하여 패치 진행

- 단, 사이트 커스텀이 있을 경우 추가 검증 기간이 증가될 수 있음.

다. 관련 문의

o 전화번호 1899-1256 또는 tech@hunesion.com로 문의 접수 진행 중