Synology NAS 보안 취약점 업데이트 권고

<학술정보원 IT운영팀, '26.10.30(금)>

❖ 최근 시놀로지 NAS 대상 랜섬웨어 침해사고가 급증 추세

❖ 시놀로지 NAS 취약점을 악용한 공격으로 확인됨에 따라 긴급 업데이트 필요

❑ 개요

❍ 시놀로지社에서 지난 9월13일 DSM 취약점을 발견하여 보안업데이트를 권고(CVE-2026-13639, CVE-2026-13684, CVE-2026-13635, CVE-2026-13673, CVE-2026-6205, CVE-2026-13666, CVE-2026-13623, CVE-2026-13683)

❍ 해당 취약점을 악용하여 DSM 관리자페이지 취약점을 악용하여 NAS 내부파일 검색 및 랜섬웨어를 통한 파일암호화 공격 실행

❍ 이에 따라 보안 업데이트 및 **특이사항 발생 시 즉시 ECSC 신고(053-714-0777, cert1@ecsc.go.kr) 및 IT운영팀 정보보안 신고(02-920-7383)**

❑ 보안 권고

❍ 영향 받는 제품 버전의 경우 업데이트 버전에 맞춰 즉시 업데이트

제품명	심각성	업데이트 버전
DSM 7.4	Critical	7.4-90075 이상 버전으로 업그레이드
DSM 7.3		7.3.2-86009-4 이상 버전으로 업그레이드
DSM 7.2.2		7.2.2-72806-9 이상 버전으로 업그레이드
DSM 7.2.1		7.2.1-69057-12 이상 버전으로 업그레이드

❍ 참고 URL : https://www.synology.com/ko-kr/security/advisory/Synology_SA_26_13