Synology NAS 대상 랜섬웨어 공격 주의 권고

□ 개요

○ 최근 Synology NAS를 대상으로 한 랜섬웨어 공격으로 저장된 파일이 암호화되는 피해가 발생하고 있어 사용자 주의 필요

○ 피해 예방을 위해 기존 보호나라 **「Synology 제품 보안 업데이트 권고」**에 따른 Synology 보안 업데이트 적용 및 아래 보안 조치 이행 권고

□ 감염 의심 징후

○ NAS에 저장된 파일이 갑자기 열리지 않거나 파일명·확장자가 비정상적으로 변경*되고 파일 복구를 대가로 금전을 요구하는 안내문 등이 나타남

* L0CK3D, locked, lock3d, lock3D 등의 유사하지만 다양한 형태의 확장자로 변경되는 사례 발생

□ 예방 및 보안 조치

○ **(보안 업데이트)** 감염 징후가 없는 장비는 제조사 안내에 따라 해당 모델에서 지원하는 최신 DSM 및 설치 패키지로 업데이트

- DSM의 세부 업데이트 번호까지 확인하고, 지원 종료 버전 사용시 지원 가능한 버전으로 전환 또는 장비 교체 검토

※ 관련 취약점·패치 정보: 보호나라「Synology 제품 보안 업데이트 권고」참고

○ **(외부 접근 제한)** NAS 관리화면의 인터넷 직접 노출을 최소화하고, 불필요한 포트포워딩·원격접속·서비스 비활성화

- 원격접속이 필요한 경우 VPN 등 통제된 접속 경로를 사용하고, 방화벽을 통해 접속 허용 대상·서비스 제한

○ **(계정 보호)** 기본 관리자 계정 비활성화, 다른 서비스와 구분되는 강력한 비밀번호 사용 및 다중인증 설정

○ **(백업 보호)** 중요 데이터는 NAS와 분리된 오프라인 저장장치 또는 변경·삭제가 제한된 백업에 보관하고 정기적인 복원 점검 시행

※ NAS에 상시 연결된 저장장치와 동기화된 데이터도 피해를 입을 수 있으므로 별도 보호 필요

□ 감염 의심 시 대응 방법

○ **(즉시 격리)** 파일 암호화・랜섬노트 등 감염 징후 발견 시 NAS의 네트워크 연결을 차단하고, 연결된 동기화・백업 작업 중단

○ **(현장 보존)** 랜섬노트・암호화 파일・시스템 및 접속 로그를 보존하고, 발견 시각・장비 모델・DSM 버전・조치 내역 기록

- 임의 초기화・포맷・재설치 및 암호화 파일 삭제・덮어쓰기 금지
- 불필요한 전원 종료・재부팅・업데이트를 피하고, KISA에 침해사고를 신고하여 피해 대응・복구 지원 요청 후 KISA의 안내에 따라 추가 피해 방지 및 증거 보존 조치 수행

○ **(복구 주의)** 출처가 불분명한 복구 프로그램의 실행이나 복구를 보장하며 금전을 요구하는 사설 복구업체 이용 주의

□ 침해사고 신고

○ ‘KISA 인터넷 보호나라&KrCERT’ 홈페이지(www.boho.or.kr)→ 침해사고 신고 → 신고하기 → 랜섬웨어

[참고자료]

[1] KISA 보호나라, Synology 제품 보안 업데이트 권고

https://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000133&menuNo=205020&nttId=72254&pageIndex=1

[2] Synology, 구버전 DSM 대상 랜섬웨어 공격 및 보안 업데이트 안내

https://www.synology.com/en-us/company/news/article/C3RB3R/Synology%20urges%20users%20to%20apply%20security%20updates%2C%20extends%20PHP2Shell%20fixes%20to%20older%20DSM%20releases