랜섬웨어 악성코드 감염피해 예방을 위한 보안강화 권고

2025. 12. 06.(토) 디지털위협대응본부

□ 개요

○ 최근 국내외적으로 React 서버 컴포넌트 취약점(CVE-2025-55182, CVE-2025-66478)* 등을 악용한 랜섬웨어 위협이 발생하고 있어 보안 담당자들의 사전 점검 및 대비 필요

* 설명 : React Server Components(RSC)에서 사전 인증 원격 코드 실행 취약점

※ KISA-보호나라 공지 - React 서버 컴포넌트 보안 업데이트 권고(`25.12.5)
https://www.boho.or.kr/kr/bbs/view.do?bbsId=B0000133&pageIndex=1&nttId=71912&menuNo=205020

□ 주요 사고사례

○ **(서버) 보안 업데이트나 설정이 미흡하여 랜섬웨어 감염 및 주요 자료 유출**

- [사례1] 클라우드서비스 회사의 React 서버 보안패치 미흡으로 감염
- [사례2] 기업 Active Directory 등 중앙관리형 솔루션 환경의 사용자 계정, 권한, 보안 정책 관리의 미흡으로 감염
- [사례3] 웹 취약점(파일 업로드 등) 및 OS 취약점을 악용하여 감염
- [사례4] 쉬운 패스워드를 사용하거나 접근제어 정책 없이 외부에서 원격 포트(22, 1433, 3389 등)로 접속하여 감염

○ **(PC) 보안 수칙을 준용하지 않아 랜섬웨어 감염 및 주요 자료 유출**

- [사례1] 공문, 이력서, 견적서 등으로 위장한 악성메일의 첨부파일(랜섬웨어) 실행
- [사례2] P2P 프로그램을 통해 다운로드 받은 최신 영화 등으로 위장된 파일(랜섬웨어) 실행
- [사례3] 취약한 버전의 브라우저를 이용해 악성코드(랜섬웨어)가 은닉된 웹사이트 방문

○ (NAS) 보안 설정이 미흡하여 랜섬웨어 감염 및 주요 자료 유출

- [사례] 접근제어 없이 공장 출하 시 설정된 기본 관리자 패스워드를 사용하거나, 보안 업데이트 미적용으로 감염

□ 대응방안

○ 외부 접속 관리 강화

- 기업 자산 중 외부에 오픈된 시스템(DB 서비스, NAS, 공유기 등) 현황을 파악하고, 불필요한 시스템*은 연결 차단
  * 특히 테스트 서버, 유휴 서버 등 방치되어 있는 시스템 점검 및 중요 시스템 접속자의 경우 개인 단말에 임의로 원격 제어 프로그램을 설치해서 사용하는지 여부도 확인 필요
- 불필요한 네트워크 서비스 중지 및 기본 서비스 포트(22, 1433, 3389 등) 사용 지양
- 외부 접속 허용이 필요한 경우 접속 IP 및 단말기기 제한, 다중인증 설정, 내부이동 차단을 위한 서버별 접근제어 설정·확인, 비정상 접속여부에 대한 주기적인 로그* 확인
  * 해외 및 야간·주말 접속 IP, 평소와 다른 일반적이지 않은 네트워크 통신량 등
  ※ 유지보수를 위한 외부업체의 접속연결은 필요시에만 허용, 상시 연결 허용 지양

○ 계정 관리 강화

- 최초 설치 시 기본 관리자 패스워드는 반드시 변경 후 사용
- 사용하지 않는 기본 관리자 계정 비활성화 및 권한 제외
- 알파벳 대문자와 소문자, 특수문자, 숫자를 조합한 복잡한 패스워드 사용
- 정기적으로 비밀번호 변경
- 계정 비밀번호 인증 이외의 추가적인 2차 인증수단 적용
- 시스템 원격 접속 계정정보 평문 저장 금지

○ 백업 관리 강화

- 중요 자료는 네트워크와 분리된 별도의 저장소*에 정기적인 백업 권고
  * 많은 피해기업이 백업을 수행하였으나, 동일 저장소에 보관함으로써 암호화되어 복구에 어려움을 겪음
  ※ 외부 클라우드 등에 중요 자료를 보관하고 소유기반의 이중인증 적용 등

- 클라우드 자체에 대한 랜섬웨어 감염을 대비하여 클라우드에 보관된 자료에 대해서도 정기적인 백업 수행

○ **이메일 사용자 보안 강화**

- 사용자는 송신자를 정확히 확인하고 모르는 이메일 및 첨부파일은 열람 금지
  ※ 가상화 기반의 격리된 네트워크 환경에서 이메일 첨부파일 내용 확인
- 이메일 수신 시 출처가 불분명한 사이트 주소는 클릭을 자제
- 첨부파일의 확장자를 확인하고 문서 아이콘으로 위장한 실행파일(.exe 등)은 클릭 자제
  ※ 윈도우 사용자의 경우, 파일 탐색기 > 보기 > '파일 확장명' 체크 상태
  ※ 파일 탐색기 > 보기 > 옵션 > 폴더 및 검색 옵션 변경 > 보기 > '알려진 파일 형식의 파일 확장명 숨기기' 체크해제 상태
- 이메일 보안 솔루션 사용으로 유해성 유무 확인 및 악성 이메일 차단

○ **이메일 시스템 관리자 보안점검**

- 비인가 계정 등록 여부 및 비정상 로그인 시도 점검
- 기존 평문으로 수발신한 메일 내용 內 시스템 계정정보 점검·변경
- 시스템 계정정보 등 민감한 정보 평문 발송 금지
- 이메일 보안 솔루션 사용으로 유해성 유무 확인 및 악성 이메일 차단

○ **Active Directory 환경 보안 강화**

- 계정 관리 강화를 위한 특권 관리자 계정 구분 사용 및 인증정보(Credential) 주기 관리
- 특권 권한 관리자 단말 보호, 접속경로 통제 강화 등 접근통제 보안 강화
- 중요 시스템의 중앙화된 로그 수집 및 모니터링(특권 관리자 인증, 비정상 서비스 설치 등)

○ **NAS 보안 강화 방안**

- 최초 설치 시, 기본 관리자 패스워드는 반드시 변경 후 사용
- 자동 업데이트를 활성화하여 최신 펌웨어 유지

- 인터넷을 통한 직접 접속은 차단하고, 사내망에서 운영 권고
  ※ 불가피한 경우, 장비의 비밀번호 관리 및 백업, 보안 업데이트 등 철저한 관리 필요

○ 기타

- 자동 업데이트를 활성화하여 운영체제, 소프트웨어 최신 보안패치 적용
- 바이러스 백신 설치 및 최신의 업데이트 상태를 유지
- 랜섬웨어 감염에 대비한 복구 계획수립 및 모의훈련 수행

□ 침해사고 신고

○ 'KISA 인터넷보호나라&KrCERT' 홈페이지(www.boho.or.kr) → 침해사고 신고

[참고자료]

(1) 랜섬웨어 대응 가이드('23년 개정본)
- 보호나라 홈페이지(www.boho.or.kr) → 알림마당 → 보고서/가이드 내 1505번 게시물

(2) 랜섬웨어 대응을 위한 안전한 정보시스템 백업 가이드(개정본)
- 보호나라 홈페이지 → 알림마당 → 보고서/가이드 내 1466번 게시물

(3) NAS 보안 가이드
- 보호나라 홈페이지 → 알림마당 → 보고서/가이드 내 1515번 게시물

(4) 중소기업 침해사고 피해지원 서비스 동향 보고서(2024년 3분기) - 랜섬웨어 동향 및 사고사례
- 보호나라 홈페이지 → 알림마당 → 보고서/가이드 내 1527번 게시물

(5) 웹에디터 보안 가이드
- 보호나라 홈페이지 → 알림마당 → 보고서/가이드 내 1491번 게시물

(6) 웹서버 보안 강화 안내서
- 보호나라 홈페이지 → 알림마당 → 보고서/가이드 내 1359번 게시물

(7) AD서버 악용 내부망 랜섬웨어 유포 사례 분석
- 보호나라 홈페이지 → 알림마당 → 보고서/가이드 내 1383번 게시물

(8) AD(Active Directory) 관리자 계정 탈취 침해사고 분석 기술 보고서
- 보호나라 홈페이지 → 알림마당 → 보고서/가이드 내 1379번 게시물