

정보관리기술사 데일리 다이제스트

2026-09-20 · 국내/국제/공공 12대 도메인 매핑

1. 오늘의 브리핑

축	도메인	헤드라인	키워드
국내	SE SW 정보보안	AI 코딩 에이전트 플러그인 공급망 취약점 근거 OWASP Top 10 for LLM Applications (공급망 취약점 항목) · AI 에이전트 플러그인 공급망 위협 확인 · dailysecu.com/news/articleView.html?idxno=208552	플러그인4셸 · 공급망보안 · 제로클릭RCE · 코드서명검증
국제	SE AI 정보보안	클로드로 오픈AI 직원 계정 탈취 성공 AI 활용 취약점 체이닝 공격 실증 · thehackernews.com/2026/09/claude-opus-5-helped-researchers-take.html	익스플로잇체이닝 · 계정탈취 · AI자동화공격 · RCE
공공·정책	LAW SE 법·규제	ISMS-P 심사기준 개선 시행령 개정 입법예고 근거 「개인정보 보호법 시행령」 개정안 (ISMS-P 심사기준 개선) · ISMS-P 인증 심사기준 제도 개선 · pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=D010030000&nttlId=12500	ISMS-P · 개인정보보호법 · 시행령개정 · 입법예고

2. 오늘의 토픽 — AI 코딩 에이전트 플러그인 공급망 보안(Plugin4Shell)

SE SW DS | 출제 예상: 2교시 | 근거: SLSA(Supply-chain Levels for Software Artifacts), OWASP Top 10 for LLM Applications

2-1. 개념 및 정의

AI 코딩 에이전트 플러그인 설치·업데이트 시 검증된 코드와 실행 코드가 달라지는 공급망 취약점. 검증 우회로 임의 코드를 삽입해 제로클릭 원격코드실행을 유발하는 위협.

2-2. 등장 배경

클로드 코드·코덱스·코파일럿 등 주요 AI 코딩 에이전트 플러그인에서 동일 취약점 발견. AI 에이전트 생태계 확산으로 플러그인 공급망이 새로운 공격 표면으로 부상.

2-3. 핵심 기술요소

분류	주요 기술요소	역할 및 메커니즘
검증 우회 메커니즘	TOCTOU, 코드서명 미검증, 해시불일치	검증본과 실행본 불일치로 변조 코드 실행
공급망보안 대응	SBOM, 코드서명, 무결성검증	구성요소 출처·무결성 추적 및 검증 체계
AI 에이전트 위협모델	제로클릭RCE, 자동실행권한, 플러그인샌드박스	에이전트 자동실행 권한 악용한 원격코드실행

2-4. 시험·실무 관점

- [SE 연계] 공급망보안 SBOM 기반 무결성 검증 체계 설계
- [SW 연계] CI/CD 파이프라인 내 코드서명·정적분석 강제화
- [AI 연계] AI 에이전트 자동실행 권한 최소화 원칙 적용

답안 필수 키워드 — Plugin4Shell / 공급망보안 / SBOM / 제로클릭RCE / 코드서명