소프트웨어 개발보안 가이드 일부개정 추진

□ 추진 배경

o 「행정기관 및 공공기관 정보시스템 구축·운영 지침」 내 ‘소프트웨어 보안약점 기준(제52조 관련)’이 개정(행정안전부고시 ‘21.1.19)됨에 따라 소프트웨어 개발보안 가이드 일부개정 추진

* 소프트웨어 보안약점 기준 : 설계단계(20개), 구현단계(49개)

□ 주요 개정내용

o 소프트웨어 보안약점 진단대상 및 절차 등이 유사한 보안약점 기준 통합(8건→4건)에 따른 개정사항 반영

(개정 전) 보안약점	(개정 후) 보안약점	가이드
XPath 삽입	XML 삽입	p.174
XQuery 삽입		
중요정보 평문저장	암호화 되지 않은 중요정보	p.226
중요정보 평문전송		
하드코드된 비밀번호	하드코드된 중요정보	p.236
하드코드된 암호화 키		
오류메시지를 통한 정보노출	오류 메시지 정보노출	p.286
시스템 데이터 정보노출		

o 중요도와 발생 빈도 등을 고려하여 추가된 신규 보안약점(6건)에 대한 보안약점 개요, 보안대책, 코드예제를 상세히 기술

신규 보안약점	설명	가이드
코드삽입	프로세스가 외부 입력 값을 코드(명령어)로 해석·실행할 수 있고 프로세스에 검증되지 않은 외부 입력 값을 허용한 경우 악의적인 코드가 실행 가능한 보안약점	p.143
부적절한 XML 외부개체 참조	적절한 검증 없이 XML 외부 개체를 참조하여 공격자의 공격 수단으로 사용되는 보안약점	p.170
서버사이드 요청 위조	서버 간 처리되는 요청에 검증되지 않은 외부 입력값을 허용하여 공격자가 의도한 서버로 전송하거나 변조하는 보안약점	p.191
부적절한 전자서명 확인	프로그램, 라이브러리, 코드의 전자서명에 대한 유효성 검증이 적절하지 않아 공격자의 악의적인 코드가 실행 가능한 보안약점	p.254
부적절한 인증서 유효성 검증	인증서에 대한 유효성 검증이 적절하지 않아 발생하는 보안약점	p.256
신뢰할 수 없는 데이터의 역직렬화	악의적인 코드가 삽입·수정된 직렬화 데이터를 적절한 검증 없이 역질렬화하여 발생하는 보안약점 *직렬화: 객체를 전송 가능한 데이터형식으로 변환 *역직렬화: 직렬화된 데이터를 원래 객체로 복원	p.310