한국컴퓨터정보학회 동계학술대회 논문집 제23권 제1호 (2015. 1)

S/W 개발 분석 단계에서 취약점

신성윤*, 신광성°, 이현창**
*°군산대학교 컴퓨터정보공학과
**원광대학교 정보 · 전자상거래학부(융복합창의연구소)
e-mail:{waver, syshin}@kunsan.ac.kr°*, hclglory@wku.ac.kr**

Vulnerability on Step of Analysis in S/W Development

Seong-Yoon Shin*, Kwang-Seong Shin°, Hyun-Chang Lee**,
*°Dept. of Computer Information Engineering, Kunsan National University
**Division Computer and Electronic Commerce(Institure of Convergence and Creativity),
Wonkwang University

● 요 약 ●

본 논문에서는 시스템의 어플리케이션 및 IT 인프라에 대한 모든 중요한 기술적 취약점 관리는 식별되어야한다는 것을 제시한다. 특히 개발 단계에서 실행 가능한 취약점 관리 방안이 도출되어야 한다. 그리고 취약점의 식별 및 분류에서 식별 및 인증, 암호화, 접근제어의 영역에서 정의되지 않은 취약점들은 기술적, 관리적, 운영적 관점에서 해당 영역(어플리케이션, IT 인프라)별로 누락 없이 정의하도록 한다.

키워드: 취약점 관리(Vulnerability Management), 식별 및 인증(Identification and Authentication)

I. 서 론

취약점이란 보유하고 있는 정보 시스템(하드웨어(PC 포함), 네트워크 장비, 운영체제, 소프트웨어, 등)의 탑재하고 있는 소프트웨어의 오류와 결함이나 설치하는데 있어서의 오류 등을 말한다.

취약점 관리란 IT 환경을 보다 더 안정적으로 운영하고 기업체들이 개별 보안 정책을 지키는지를 계속해서 감시하고 대응하여 위협을 완화시켜 사업의 연속성과 가용성을 가능하도록 하는 것이다.

II. 관련연구

취약점 관련 논문을 보면, [1]에서는 보안 취약점 관리업무의 문제점을 소개하고, 최근 대기업을 중심으로 활발히 구축이 추진되고 있는 웹 기반의 취약점 진단 통합관리 체계의 개념, 기능 및 운영 프로세스를 소개한다.

[2]에서는 산업 제어 시스템에서 통상적으로 발견되는 취약점은 우선순위, 발생빈도 및 영향의 심각성들과는 무관하게 정책 및 절차, 플랫폼 및 네트워크 등으로 분류된다고 하였다.

[3]에서는 정보보안 관리체계에 따라 모바일 오피스에서 위협, 취약점을 모바일 오피스 구성항목의 유형별로 분석하고 현재 기술수준에서 통제가능성을 제시하고 있다.

III. 취약점 관리 원칙과 식별 및 분류

1. 원칙

시스템의 어플리케이션 및 IT 인프라에 대한 모든 중요한 기술적 취약점 관리는 식별되어야하며 개발 단계에서 실행 가능한 취약점 관리 방안이 도출되어야 한다.

2. 식별 및 분류

식별 및 인증, 암호화, 접근제어의 영역에서 정의되지 않은 취약점들은 기술적, 관리적, 운영적 관점에서 해당 영역(어플리케이션, IT 인프라)별로 누락 없이 정의한다.

IV. 취약점 관리 대응방안 선택

식별된 취약점의 대응여부를 판단하고, 해당 취약점을 제거하기 위한 대응방안을 기본적인 대응방안, 강화된 대응방안, 엄격한 대응방안 등의 단계적 대응 관점에서 정리하여 최종적인 대응방안을 선택한다.

표 1. 취약점 대응방안 선택

취약점 (예시)	취약점 대응 단계			단계 선택
	1단계	2단계	3단계	
SQL Injection	시큐어 코딩 실시	자동화 된 소스코드 점검	네트워크에서 공격 사전 필터링	2단계
DB 권한설정 미흡	자체 권한설정 및 검토	자동화 된 권한설정 분석	n/a	1단계
불필요한 서비스 구동	정기적 자체 점검	자동화 된 불필요 서비스 탐지 및 경고	네트워크에서 서비스 모니터링	3단계

V. 취약점 관리의 사례

취약점 관리의 사례를 R사의 개발 단계 보안 요건 중 취약점 관리의 사례를 들도록 하였다. 먼저, 우선 취약점 관리의 사례로서 입력값 검증의 사례(표 2)를 들어 보도록 한다.

표 2. 입력값 검증의 사례

요건 ID	요건명	NUM	상세요건
00-00-01	입력값 검증	1	입력되는 데이터의 필터링 (Black-listing) - 명령어 행에 대한 입력값 필터링 - DB 쿼리문에 대한 입력값 필터링 ※ 필터링 세부목록은 '어플리케이션 보안 아키텍처'의 '입력값 검증' 참조
		2	허용 가능한 입력값 정의 (White-listing) - 허용 가능한 최대 또는 최소값 점검 - 허용 가능한 문자 형태 정의 - 기 정의된 값들로 부터의 선택
		3	입력값을 재확인 한다. - 예: 비밀번호 생성 시 두 번 반복 입력 등
		4	사용자가 입력한 값에 대해 서버측에서 검증을 수행하도록 한다.

V. 결론

본 논문에서는 제시하는 점은 시스템의 어플리케이션 및 IT 인프라에 대한 모든 중요한 기술적 취약점 관리는 식별되어야하고 개발 단계에서 실행 가능한 취약점 관리 방안이 도출되어야 한다는 것이다. 취약점의 식별 및 분류에서 개발 단계의 식별 및 인증, 암호화, 접근제어의 영역에서 정의되거나 다루지 않은 취약점들은 기술적, 관리적, 운영적 관점에서 해당 어플리케이션 및 IT 인프라 별로 누락이나 예외 없이 정의하도록 한다.

참고문헌

[1] Moon Ho-Gun, Park Sung-Cheol, "Development of Vulnerability Assessment Integrated Management System for Security Enhancement of Enterprise ," KICS(Information and Communication) Vol. 31 No. 5, pp. 39-45, 2014.5

[2] Kim Do-Yeon, "Vulnerability Analysis for Industrial Control System Cyber Security," JKIECS, Vol. 9, No. 1, pp. 137-142, 2014

[3] Young Jin Choi, Jong Hei Ra, Dong Ik Shin"The Exploratory Study on Security Threats and Vulnerabilities for Mobile Office Environment," The Journal of Information Technology and Architecture, Vol. 11 No. 2, pp. 175-185, 2014