무인기 지상통제체계 서버 보안취약점 조치 사례에 관한 연구

김태엽, 고정환, 권순영*
LIG 넥스원, *국방과학연구소
taeyeop.kim@lignex1.com, kojh2010@lignex1.com, *ksy2020@add.re.kr

A Study on the Sever Security Vulnerabilities for UAV Ground Control Systems

Kim Tae Yeop, Go Jeong Hwan, Kwon Soon Young*
LIG Nex1, *Agency for Defense Development(ADD)

요 약

최근 정보통신기술 및 해킹기술이 발전하여 서버 보안과 관련 하여 여러 취약점이 나타나고, 이들 취약점들을 이용하여 개인정보 침해, 도용, 서버 거부 공격 등의 보안 사고가 증가하고 있다. 그에 따라 무인기 지상통제체계 에서도 서버 보안 취약점에 대한 관리가 필요하다. 본 논문에서는 무인기 지상통제체계에서 수행한 정보보호 시험의 하나인 서버 보안 취약점 조치 사례를 통해 보안 취약점 이슈, 평가도구, 시험 목적 및 항목. 점검 및 조치 결과를 정리 하였다.

Ⅰ. 서 론

정보보안 분야가 발전하면서 취약한 보안 시스템으로 인한 여러 보안 위협 이 증가하였다. 취약한 보안 설정으로 발견된 취약점을 통해 개인정보 유출, 시스템이 직접적인 공격, 악성프로그램 삽입 공격 등 다양한 공격이 이루어진다. 무인항공기를 컨트롤 하는 지상통제체계 (GCS: Ground Control System)에서도 여러 보안 위협으로 부터의 약점에 대해 관리 및 조치가 이루어 져야 한다. 본 논문에서는 국방정보시스템 보호기준 및 보호요구항에 따른 정보시스템 보호기준 중 서버보호와 관련해 시험 평가 전 자체적으로 수행한 무인기 지상통제체계의 서버 보안 취약점 시험 도구 및 항목 그리고 점검 결과에 따른 조치 내용에 대해서 기술 하였다.

그림 1 정보시스템 보호기준

Ⅱ. 본론

1. 서버 보안취약점 이슈

취약점 분석 및 평가는 관리적, 물리적, 기술적 점검항목에 대한 취약여부를 점검하여, 악성코드 유포, 해킹 등 사이버 위협 대응을 위한 종합적 개선 과정에 해당한다. 서버 보안취약점 점검을 수행함에 있어 기술적 점검은 시스템에 대한 실제 보안값 설정에 관한 것으로 각 시스템에 대한 명령어 코드(Command), 메뉴 구성(UI)과 같은 기술적인 사항을 사전에 알아야만 가능하다. 하지만 서버 취약점 평가도구를 사용한다면 자동으로 서버에 대한 기술적 취약점 진단을 수행하고, 도출된 위험에 대한 보호대책을 제시함으로써, 그로 인한 침해사고 발생 위험을 낮추고 보안수준을 제고 할 수 있다.

2. 서버 보안취약점 평가도구

무인기 지상통제체계의 서버 보안취약점 평가도구로는 Nile SOFT사의 Secuguard SSE(System Security Explorer)를 사용하였다. 시스템의 보안 취약점을 자동으로 점검하고 발견된 문제들에 대한 해결방법을 제공하여 해킹과 컴퓨터 범죄들을 예방할 수 있는 시스템 보안 취약점 평가도구다. 점검대상 시스템 내부에 점검용 에이전트를 설치 실행하여 알려진 취약점들을 사용자가 보다 쉽게 접근하고 사용자가 적절한 조치를 취할 수 있게 상세한 취약점 정보를 제공하며 내외부 해킹으로부터 안전한 시스템을 유지할 수 있도록 보안 무결성을 제공한다. 아래 그림 2는 Secuguard SSE 평가도구를 이용했을 때 진단 및 결과의 예시를 보여준다.

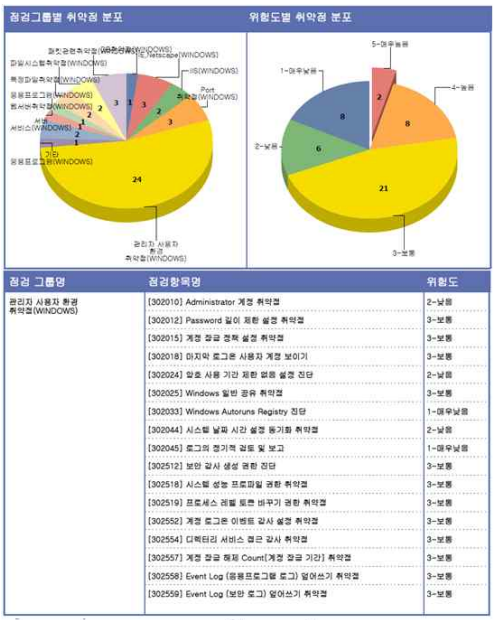

그림 2 Secuguard SSE 진단 및 결과 보고서

3. 서버 보안취약점 시험 목적 및 항목

무인기 지상통제체계의 정보보호 서버 보안취약점 시험은 정보시스템 구축/운영 중 체계 형상의 변경에 따라 발생할 수 있는 보안 위협 및 취약점을 식별, 대응하여, 체계의 안전성, 보안성을 유지하는데 목적이 있다. 서버 보안취약점 시험 내용은 국방사이버안보훈령에 따라 평가 진행 되었으며 무인기 지상통제체계 內 구축된 서버에 대한 보안취약점 항목 조치 여부를 확인 하였다.

4. 서버 보안취약점 점검 결과

무인기 지상통제체계의 서버 보안취약점 조치 대상이 되는 장치는 총 15개의 장치이다. 아래 그림 3과 같이 각 서버별 사전수행 취약점 조치 항목의 개수가 다르게 점검되었고 보안 취약점 중요도에 따라 5단계로 구분되어 점검되었다.

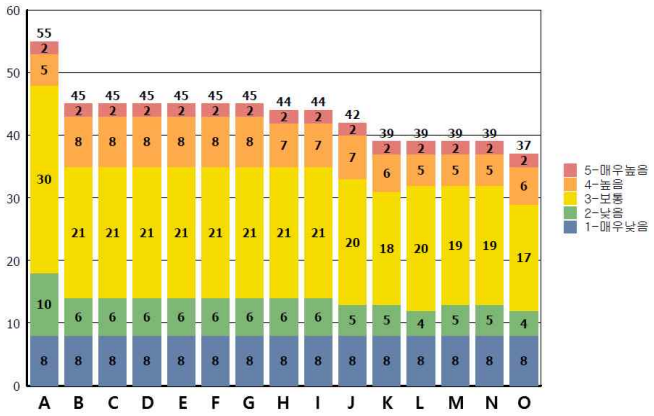

그림 3 Secuguard SSE 진단 결과 보고서

무인기 지상통제체계 내에서 서버 보안취약점 점검 대상으로 분류된 장치는 H/W의 경우 HP ProLiant MicroServer Gen8 제품을 사용하였고 OS로는 Windows Server 2012 R2를 사용 했지만 각 장비 및 장치별 용도에 따라 보안 취약점 항목이 통제장비와 장치별로 다르게 식별되었다.
공통적인 항목은 Windows 계정 및 비밀번호, 계정 잠금 정책, Autoruns Registry 진단, 시스템 시간동기화, 계정 로그온 및 잠금 해제, 로그 정책, 로그 덮어쓰기, Windows 권고 사항 미적용, 바이러스 백신, Windows 보안 드라이버 및 패치 업데이트, 네트워크 진단 등의 취약점 항목이 분석되었다. 각 장치별 운용 환경에 따라 설치된 어플리케이션의 영향으로 각 장치별 취약점 항목의 차이를 보였으며 또 체계 개발 기간 개발자가 설치한 어플리케이션이나 설정 등에 따라서도 보안 취약점이 다르게 분석되었다. 아래 표 1은 무인기 지상통제체계 장치별 세부 보안취약점 결과 총 80건 중 일부 내용 및 세부 항목 별 중요도 레벨을 보여준다.

표 1 무인기 지상통제체계 장치별 취약점 내용

보안취약점 항목	레벨
[302010] Administrator 계정취약점	2-낮음
[302012] Password 길이제한설정취약점	3-보통
[302013] 상반된 권한 위험 취약점	2-낮음
[302014] 관리자 권한 사용자 진단	3-보통
[302015] 계정 잠금 정책 설정 취약점	3-보통
[302018] 마지막 로그온 사용자 계정 보이기	3-보통
[302020] 한번도 로그온 하지 않은 계정 진단	2-낮음
[302022] '계정 사용 안함' 설정되어 있는 계정 취약점	2-낮음
⋮	⋮
[302023] 최근 암호 기억 미설정 취약점	3-보통
[302024] 암호 사용 기간 제한 없음 설정 진단	2-낮음
[302025] Windows 일반 공유 취약점	3-보통
[302033] Windows Autoruns Registry 진단	1-매우낮음
[316211] Internet Explorer 최신 패치 취약점	5-매우높음
[317057] IIS 링크 사용금지 취약점	4-높음
[317059] IIS 데이터 파일 ACL 적용 취약점	4-높음
[317063] IIS CGI 실행제한 설정 취약점	4-높음
[317064] IIS 서비스 구동 점검	3-보통
[317073] IIS 오류 메세지 관리 취약점	2-낮음

5. 서버 보안취약점 조치 결과

서버 보안취약점 평가도구 Secuguard SSE를 사용해서 진단 받은 내용을 바탕으로 무인기 지상통제체계의 총 15개 장치에 대해 시험 평가 전 자체적으로 서버 보안취약점 조치를 수행 후 재진단을 통해 취약점 항목의 개수가 줄어드는 것을 확인하였다. 무인기 지상통제체계의 운용 및 시스템 특성상 조치하지 못하는 경우에 대해서는 부분적으로 적용하였다. 특히, 대부분의 패치 및 업데이트 항목은 시스템에 기 개발된 시스템에 문제를 발생 할 가능성이 있고 무인기 지상통제체계는 외부 망을 사용하지 않는 단독 망에서 운용됨에 따라 조건부 조치하였다.

Ⅲ. 결론

본 논문에서는 무인기 지상통제체계의 서버 보안취약점 조치 사례를 통해 정보보호 서버 보안취약점 시험평가 계획 수립 시 필요한 서버 보안취약점 이슈 및 평가도구, 서버 보안취약점 시험 목적 및 평가 항목, 서버 보안취약점 점검 및 조치 결과에 대하여 기술하였다.
정보보호시험은 추후 이어지는 모든 국방 사업에서 필수적으로 요구될 사안이므로, 본 서버 보안취약점 조치사례가 타 사업의 참고자료로 유용하게 활용될 수 있기를 기대한다.

참 고 문 헌

[1] 국방부, “국방 정보화업무 훈령”, 제2436호, 2020. 06

[2] 방위사업청, “상호운용성 관리지침”, 제569호, 2019. 09

[3] 한국인터넷진흥원, “주요 정보통신 기반시설 기술적 취약점 분석·평가 방법 상세가이드”, 2017