권한 상승 취약점 점검 가이드 및 탐지 방법 제안

장재훈*, 고동의**, 정찬유***, 고기완****, 김도현****

*숭실대학교, **순천향대학교, ***한국디지털미디어고등학교, ****스틸리언

Privilege Escalation Testing Guide and Vulnerability Detection Method

Jae-Hoon Jang*, Dong-Ui Go**, Chan-Yoo Jeong***, Gi-Wan Go****, Do-Hyun Kim****

*Soongsil University, **Soonchunhyang University, ***Korea Digital Media High School, ****Stealien

요 약

권한 상승 취약점은 시스템과 애플리케이션에 대한 액세스 권한을 획득하여 관리자가 의도한 것보다 높은 수준의 권한을 탈취하며 시스템 환경에 심각한 영향을 끼칠 수 있다. 권한 상승 취약점은 운영체제, 드라이버, 시스템 설정, 소프트웨어 등 넓은 영역에서 발생할 수 있기 때문에 사전에 이를 방지하고 점검하는 권한 상승 취약점에 대한 방어대책이 필요하다. 본 논문은 기존 보안 취약점 점검 가이드와 취약점 사례 분석을 통해 도출한 점검 항목을 바탕으로 권한 상승 취약점 점검 가이드를 제시하고 이를 기반으로 한 권한 상승 취약점 탐지 방법을 제안한다.

I. 서론

권한 상승 취약점은 공격자가 사용자에 대해 보호되는 자원들에 접근할 수 있고 개발자나 시스템 관리자가 의도한 것보다 높은 수준의 권한을 얻어서 허가되지 않은 행동을 할 수 있는 결함이다. 한국인터넷진흥원의 2021년 사이버 위협 전망 보고서에 따르면, 글로벌 전망과 국내 사이버 위협 인텔리전스 전망 총 13가지 항목에서 랜섬웨어, 악성 이메일 등 악성코드 위협과 APT 공격 위협이 7가지 항목을 차지했다. [1]

이런 공격의 공통점은 권한 상승 취약점이 필요한 것이다. 하지만 원격 코드 실행(RCE, Remote Code Execution) 취약점과 비교하여 개발자나 방어자는 권한 상승 공격을 간과하는 경우가 많다. [2]

현재의 시스템은 임의의 코드 실행을 초래할 수 있는 취약점에 초점을 맞추고 시스템에 대한 액세스 권한을 획득하지 못하게 방지하는 방법으로 발전됐다. 하지만 기술이 발전하며 공격자가 시스템에 접근할 수 있는 수많은 방법이 있고, 단순한 원격 코드 실행 취약점만으로 시스템을 완전히 장악하기 힘들다. 최근에는 원격 코드 실행 취약점뿐만 아니라 완전한 시스템 접근을 위한 권한 상승 취약점을 결합한 공격 체인이 요구된다. 취약점 매입 플랫폼인 제로디움(Zerodium)은 안티바이러스 로컬 권한 상승, 윈도우 권한 상승, VMWare Virtual Machine Escape 취약점에 각각 1만 달러, 8만 달러, 20만 달러를 제공하고 있다. 프로세스가 샌드박스로 처리되는 브라우저 및 모바일 운영체제와 같이 업체에서 구매하는 많은 프로그램에 대한 공격 체인의 많은 부분에서 권한 상승과 결합된 RCE가 필요하다. [2]

권한 상승은 일반적으로 공격자의 최종 목표는 아니지만, 보다 구체적이고 치명적인 사이버 공격을 위해 자주 사용되어 공격자가 악성코드를 배포하거나 보안 설정을 수정하여 피해 시스템에서 추가 공격 벡터를 만들 수 있다. 또한, 다른 사용자의 민감한 개인 정보를 노출하거나 접근 로그를 삭제하여 자신의 흔적을 지울 수도 있다. 따라서 권한 상승 취약점은 치명적인 공격을 유발하며 이에 대한 방어 대책도 필요한 시점이다.

한국인터넷진흥원에서 제공하는 국내 정보보호 기술안내서 가이드에는 모바일 앱 소스코드 검증 가이드, 드론 사이버보안 가이드 등 다양한 종류가 있지만 권한 상승에 관련된 내용을 찾아보기 힘들다. [3]

다른 취약점 체크리스트나 점검 문서 등에서는 전반적인 시스템 보안과 취약점 점검, 보안 평가 관련 내용만 찾아볼 수 있다. 이처럼 권한 상승 취약점에 중점을 둔 보안 대책 및 보안 가이드는 찾기 힘들다. 해외 자료에서는 MITRE ATT&CK Framework 중

권한 상승 관련 내용이 있지만, 다양한 공격기법들에 대한 정보를 분류해 목록화한 데이터만 존재하기 때문에 실무에 곧바로 적용하기 힘들다. 권한 상승 공격은 시스템 보안 설정만으로 많은 권한 상승 위협으로부터 보호할 수 있는 만큼 점검 가이드를 제공하는 것만으로도 많은 위협과 피해를 예방할 수 있다.

II. 권한 상승 취약점 점검 가이드

본 논문에서는 기존 보안 취약점 점검 가이드와 권한 상승 관련 자료, 다양한 원데이 권한상승 취약점 사례를 분석하고 참조하여 Windows와 Linux 환경에서 각각 10가지 항목을 통해 권한 상승 취약점을 점검할 수 있는 가이드를 작성했다.* 한국인터넷진흥원의 기술안내서 가이드들을 참고하여 취약점 점검 가이드의 틀을 구성했다.

MITRE ATT&CK Framework Enterprise의 Privilege Escalation 분류를 확인하여 13가지의 대표적인 공격 방법과 기존의 권한 상승 관련 체크리스트 항목을 조사해 점검 가이드에 포함했다. 점검 가이드는 항목별로 취약점 개요, 취약점 점검 방법, 공격 방법의 순서로 구성하여 실무에 바로 적용할 수 있도록 작성했다. [4]

1	리눅스 권한 상승 점검 방법
1.1	취약한 커널
1.2	관리자 권한 프로그램
1.3	취약한 소프트웨어
1.4	잘못된 비밀번호 관리
1.5	취약한 내부 서비스
1.6	잘못된 권한 설정
1.7	sudo 권한 남용
1.8	잘못된 환경변수 설정
1.9	Cronjob
1.10	Unmounted 파일 시스템
2	윈도우 권한 상승 점검 방법
2.1	저장된 크리덴셜
2.2	DLL 하이재킹
2.3	Unquoted 서비스 경로
2.4	약한 폴더 권한 설정
2.5	약한 서비스 권한 설정
2.6	약한 레지스트리 권한 설정
2.7	Always Install Elevated
2.8	Autorun 수정
2.9	Tater / Hot Potato
2.10	토큰 조작

[표 1] 권한 상승 취약점 점검 항목

* 장재훈, 고동의, 정찬유, 고기완, 김도현, 권한 상승 취약점 점검 가이드, (https://bit.ly/3jp1Wlg)

권한 상승 취약점 점검 목록은 크게 논리적 취약점, 기술적 취약점, 시스템 권한 설정으로 나눠서 점검 항목을 작성했다. 리눅스에서의 논리적 취약점의 경우, 최근 발생했던 sudo 권한상승 취약점(CVE-2021-3156)과 polkit 권한상승 취약점(CVE-2021-3560) 등 취약한 소프트웨어나 내부 서비스에서 발생 가능한 취약점 점검 목록을 기술했다. 기술적 취약점은 DirtyCow (CVE-2016-5195) 취약점과 Netfilter 권한상승 취약점(CVE-2021-22555) 등 리눅스 커널에서 발생한 원데이 권한 상승 취약점을 분석하고 익스플로잇 방법을 점검 가이드에 포함했다. 시스템 권한 설정은 잘못된 비밀번호 관리, 잘못된 권한 설정 등으로 발생 가능한 권한 상승 공격을 점검하는 방법을 기술했다. 윈도우에서도 마찬가지로 약한 레지스트리, 서비스 권한 설정 등 논리적인 취약점과 DLL 하이재킹, 토큰 조작 등 기술적인 취약점, Autorun, Always Install Elevatd 등 시스템 권한 설정에서 발생 가능한 다양한 범주의 권한 상승 취약점, 공격 사례를 분석하고 정리했다.

III. 가이드 기반 상세 탐지 방법

권한 상승 취약점 점검 가이드는 넓은 영역에서 발생 가능한 공격벡터를 점검할 수 있는 방법을 제시한다. 시스템 보안 설정, 약한 권한 관리뿐만 아니라 취약한 프로그램을 식별하고 새로운 제로데이 취약점을 발견하여 사전에 위협을 방어할 수 있다. 점검 가이드를 활용해 권한 상승 취약점을 탐지하는 상세한 방법을 기술한다. 가이드 중 적용한 항목은 윈도우 권한 상승 점검 방법의 "2.2. DLL 하이재킹", "2.3. Unquoted 서비스 경로", "2.4. 약한 폴더 권한 설정"이다.

1. DLL 하이재킹

DLL(Dynamic Link Library)은 윈도우에서 구현된 동적 라이브러리다. 소프트웨어 개발에서 자주 사용하고 기초적인 함수들을 중복 개발하는 것을 피하기 위해 표준화된 함수 및 데이터 타입을 만들어서 다른 프로그램이 불러서 쓸 수 있다. 윈도우 프로그램에서 DLL을 참조할 때, 지정 경로에 DLL의 유무를 확인한다. 만약 DLL이 없다면, 프로그램이 참조하는 지정 경로에 악성 DLL을 배치함으로써 권한 상승을 할 수 있다. 보통, 윈도우 프로그램은 DLL를 찾기위해 사전에 정의된 검색 순서를 이용하고 특정 순서에 따라 경로를 확인한다.

1	Application이 로드된 디렉터리
2	System 디렉터리
3	Windows 디렉터리
4	현재 작업 디렉터리
5	PATH 환경변수 디렉터리

[표 2] DLL 경로 탐색 순서

대표적인 윈도우 권한상승 취약점 도구인 PowerUp 을 이용해 DLL Hijacking 취약점을 탐지할 수도 있다. 보통 PowerUp 도구의

Write-HijackDll 기능을 이용해 악성 DLL 파일을 작성한다. 취약한 프로그램이 시작할 때, 작성한 악성 DLL을 로드하여 상승된 권한으로 원하는 명령이나 코드를 실행할 수 있다. 일반적으로 다음과 같은 과정을 통해 DLL Hijacking 취약점이 존재하는지 확인한다.

1.1. 잘못된 DLL 경로의 프로세스 탐색

DLL Hijacking을 통한 권한상승을 위해 첫 번째로 분석해야할 부분은 SYSTEM 권한이나 타사용자의 권한으로 동작하고 있는 프로세스의 목록 중, 잘못된 DLL 경로(존재하지 않는 폴더, 잘못된 파일 이름 등)를 참조하는 프로세스를 찾는 것이다. Process Monitor 도구의 필터링 기능을 이용하여 쉽게 프로세스를 검색할 수 있다. [5]

1.2. 폴더 권한 확인

소프트웨어의 설치 경로가 C:\Program Files가 아닌, C:\[Directory]라면 일반사용자도 해당 디렉터리에 접근할 수 있다. 추가적으로 Perl, Python, Ruby와 같은 프로그램은 PATH 환경변수에 보통 추가된다. 공격자는 해당 디렉터리에 악성 DLL을 배치하거나 기존 DLL 파일을 변조하여 권한상승할 수 있는 기회를 만들 수 있다. 만약, 관리자 권한의 프로세스에서 해당 디렉터리의 DLL을 참조한다면 정상적인 코드가 실행되지 않고 공격자가 작성한 공격 코드가 상승된 권한으로 작동할 것이다.

위와 같은 점검을 통해 DLL 하이재킹 취약점이 식별되면, 공격 코드를 DLL로 작성해서 하이재킹하면 권한 상승할 수 있다.

2. Unquoted 서비스 경로

서비스가 시작하면 윈도우는 프로그램을 실행하기 위해 검색한다. 만약, 바이너리의 경로가 unquoted라면 윈도우는 프로그램을 시작 경로부터 모든 폴더를 검색한다. 특정 서비스의 경로가 "(큰따음표), '(작은따음표)로 묶여있지 않고, 공백이 포함되어 있고, 해당 경로에 쓰기 권한이 있다면 권한 상승할 수 있다.

"C:\Program Files\Unquoted Path\service.exe"라는 서비스가 있다고 가정하고, 해당 서비스를 실행할 때 unquoted되어 있다면 윈도우에서는 다음과 같은 순서로 검색한다.

1	C:\Program.exe
2	C:\Program Files\Unquoted.exe
3	C:\Program Files\Unquoted Path.exe
4	C:\Program Files\Unquoted Path\service.exe

[표 3] Unquoted 서비스 경로 탐색 순서

이러한 이유로 공격자는 "C:\Program Files\Unquoted.exe" 나 "Unquoted Path.exe"를 만들어서 권한상승할 수 있다.

3. 약한 폴더 권한 설정

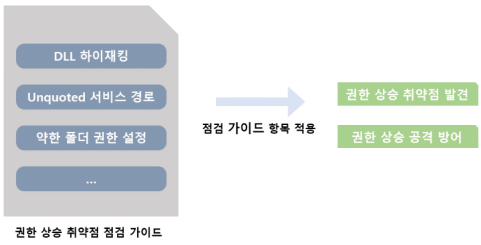
사용자가 특정 서비스의 폴더에 쓰기 권한을 가졌다면 프로그램 파일을 악성 프로그램으로 바꿀 수 있다. 서비스가 다시 시작할 때, 미리 바꿔 둔 악성 프로그램을 실행할 수 있고, 서비스가 타 사용자의 권한이나 더 높은 권한으로 실행되어 권한 상승할 수 있다.

4. 점검 가이드 적용 및 취약점 탐지

위와 같은 점검 가이드 내용을 국내에서 사용되는 여러 프로그램 대상으로 프로세스 모니터 도구를 이용하여 점검했다. [6]

프로세스 모니터의 필터링 기능을 이용해서 잘못된 DLL 경로를 탐색하는 프로세스를 찾아 DLL 하이재킹 취약점을 분석하거나 Unquoted하게 서비스 경로를 설정하여 잘못된 프로그램을 검색하는 프로세스를 통해 권한 상승 취약점을 분석했다. (Result contains NOT FOUND 등의 필터링 조건으로 설정) 또한, Integrity Level을 필터링해서 High나 SYSTEM 권한으로 동작하는 프로세스 중, 약한 폴더 권한 설정으로 프로그램을 바꿔치기 할 수 있는 서비스를 찾아가며 권한 상승 취약점을 분석했다. [7]

점검 가이드를 적용해서 취약점을 분석한 결과, 3건의 권한 상승 취약점을 발견했고 일반 사용자가 관리자 권한을 획득할 수 있었다. 현재 해당 취약점들은 한국인터넷진흥원에 신고한 상태다. 넓은 영역에서 발생 가능한 권한 상승 취약점 중, 프로그램을 대상으로 분석했음에도 불구하고 쉽게 취약점을 발견할 수 있었다. 권한 상승 취약점 점검 가이드의 더 많은 항목을 적용하여 활용한다면 사전에 권한 상승 공격을 방어할 수 있을 것이다.



[그림 1] 권한 상승 취약점 점검 가이드 활용

IV. 결론

많은 사람들은 시스템에 직접적으로 접근하기 위한 해킹 공격에 대해 집중적으로 대응책을 마련한다. 시스템에 직접적으로 접근 후, 특정 행위를 하기 위해 권한이 필요한 경우가 많으며 이를 위해 권한 상승 취약점을 이용하여 높은 권한을 얻는 공격을 수행한다. 만약 시스템 환경의 보안이 확보되지 않았다면 시스템을 장악당하게 된다. 그러나 권한 상승 취약점에 대한 체계적인 보안 대책은 없는 실정이다.

이에 대한 대응 방안으로 본 논문에서는 권한 상승 취약점 점검 가이드를 제안하여 개발자나 서비스 관리자가 점검해야 할 부분에 대해 제시를 한다. 권한 상승 취약점은 고정된 영역이 아닌 넓은 영역에서 발생하기에 논리적, 기술적 취약점 항목과 잘못된 시스템 설 및 관리까지 다양한 범주에 해당하는 취약점을 점검할 수 있도록 가이드를 제시한다. 이 가이드를 기반으로 국내 프로그램을 대상으로 취약점 점검을 수행한 결과, 3건의 권한 상승 취약점을 발견하여 가이드에 대한 효율성을 입증했다. 추후 더 많은 권한 상승 취약점 사례와 점검 항목을 수정 및 보완하며 지속해서 가이드 개선 작업을 수행할 계획이다.

[참고문헌]

[1] KISA, 2021년 사이버 위협 전망, (https://www.krcert.or.kr/data/reportView.do?bulletin_writing_sequence=35878)

[2] ITWORLD, "권한 상승이 공격자에게 중요한 취약점인 이유", 2020.07, (https://www.itworld.co.kr/news/158098)

[3] KISA, KISA보호나라&KrCERT 홈페이지, (https://www.kisa.or.kr/public/laws/laws3.jsp)

[4] 정성욱, 박남제. MITRE ATT&CK Framework를 활용한 주요정보통신기반시설 기술적 취약점 점검 방안. 한국정보기술학회 종합학술발표논문집(한국정보기술학회) 2021, (), 267-269.

[5] 배재건, 공성현, 석병진, 이창훈. Windows 관리자 권한 획득을 위한 시스템 실행 파일의 DLL Hijacking 취약점 분석. 한국정보처리학회 학술대회논문집 2019, 26(1): 170-173.

[6] Microsoft, Process Monitor, (https://docs.microsoft.com/en-us/sysinternals/downloads/procmon)

[7] Vetle Økland, 2019.05, Finding Privilege Escalation with Procmon, BSides Oslo, Oslo