공개 오픈소스의 보안 취약성에 대한 학부생의 인식조사 연구

강태임*, 최창빈*, 김가연*, 이태현*, 이경호*, 조세나*, 장영수*
*한국폴리텍대학 안성캠퍼스 스마트소프트웨어과
e-mail : s6513202, cckdqlsa, 09gayeon28, mbcgo12, ghdi827, jyskkh{@naver.com}, sn3719@hanmail.net

A Study on the Awareness of Open Source Security Vulnerabilities

TaeIm Kang*, ChangBin Choi*, GaYeon Kim*, TaeHyeon Lee*, GyeongHo Lee*, Sena Cho*, YoungSu Jang*
*Dept. of Smart Software, Korea Polytechnic Ansung College

요 약

오픈소스는 소스코드를 무료로 공개하여 누구나 쉽게 사용하고 공유 할 수 있도록 만든 소프트웨어 이다. 누구나 열람할 수 있는 오픈소스의 특성상 보안에 취약하고 소프트웨어의 구조적 오류가 발생 할 수 있다. 필요한 기능을 손쉽고 편리하게 사용할 수 있다는 장점이 있지만, 검증되지 오픈소스는 해커와 같은 외부 공격에 취약점을 노출시킬 수 있다. 본 논문에서는 이러한 오픈소스의 취약점을 Adobe Flash Player의 사례를 통해 알아보고 취약점 해결방안을 고찰해 봄으로써 오픈소스를 사용하면서 발생할 수 있는 문제점을 보완하고자 하였다.

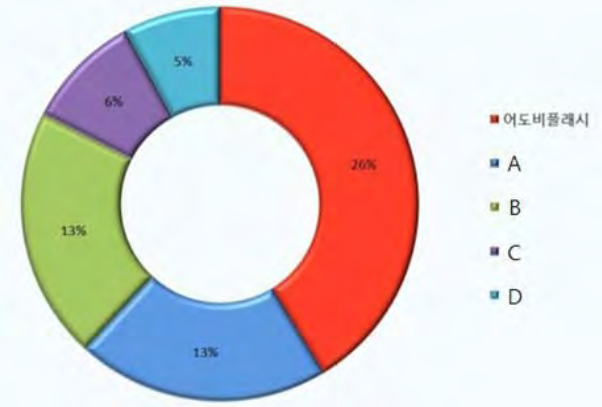
1. 서론

OSS(Open Source Software) 라고 불리는 오픈소스는 소프트웨어 혹은 하드웨어 제작자의 권리를 지키면서 원시코드를 누구나 열람할 수 있도록 한 소프트웨어 혹은 라이선스에 준하는 모든 통칭을 일컫는다[1]. 하지만 이렇게 공개된 모든 소스코드들이 오픈소스인 것은 아니다. 예를 들어, 마이크로소프트는 전체 비율로 보았을 때 극소수의 고객(예: 정부, 대학교 등)들에게만 윈도우의 소스코드를 공개했다. 오로지 보안 유지를 위해서만 소스코드를 직접 수정할 수 있으며, 그 수정 본을 재배포하는 것은 금지하였다. 이것은 오픈소스의 취지에 어긋나므로 이러한 경우는 오픈소스라 부르지 않는다. 일반적으로 소프트웨어를 개발을 할 때 필요한 기능의 오픈소스를 사용하면 개발 시간이 단축되지만 꼭 좋은 것만은 아니다. 소스코드가 모두 공개되어 있는 만큼 오픈소스는 보안 취약성(Security Vulnerability)이 드러나기 쉽고 단기적으로 얻을 수 있는 경제적 효과에만 집중하는 경향이 있으며, 이를 해커가 악용할 수 있기 때문에 보안 강화에 관심을 가지고 주의를 기울여야 하며, 검증된 오픈소스를 사용하는 습관을 가지는 것이 중요하다[2].

2. 관련연구

대학에서 학부생들이 많이 사용하는 오픈소스 관련 프로그램으로는 대표적으로 어도비 시스템즈에 인수합병된 매크로미디어사가 만든 Adobe Flash Player를 들 수 있다. Adobe Flash Player는 애니메이션, 게임, 음악 재생 기능을 포함한 콘텐츠를 생성하거나, 액션 스크립트를 이용하여 동적인 움직임이 가능한 웹 사이트를 만들 수 있기 때문에 많은 개발자들이 사용하고 활용도가 높은 오픈소스이다[2]. Adobe Flash Player의 장점으로는 응용프로그램이 많은 브라우저와 호환이 되며, 웹사이트를 더욱 표현적이고 상호 작용하게 만드는 데 도움이 된다. 단점으로는 플래시 기술을 사용하는 웹 사이트는 그렇지 않은 웹사이트보다 느려지는 경향이 있으며, 플래시 무비를 보려면 Adobe Flash Player를 설치해야한다[3]. 그리고, 무엇보다도 Adobe Flash Player의 소스 공개로 인해 보안에 취약할 수 있는 제로데이(Zero-day) 보안 취약점이 발견되었다[4]. 제로데이 보안 취약점은 컴퓨터 소프트웨어의 취약점을 공격하는 기법으로, 해당 취약점에 대한 보안 패치가 나오지 않은 시점에서 이루어지는 공격을 말한다[5]. Adobe Flash Player의 제로데이 보안 취약점은 플래시 실행용 SWF파일을 포함한 마이크로소프트 엑셀 문서를 열면 원격 관리 도구

ROKRAT을 다운로드하고 시스템 메모리에서 실행된다. 이후 ROKRAT이 실행된 시스템은 해커가 자기 의지대로 제어할 수 있다.



(그림 1) 고위험군 보안 취약 소프트웨어 예시[6]

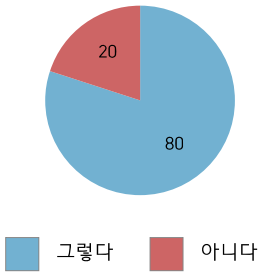
이렇듯 프로그램 코드(Code)의 품질은 프로그램 보안, 유지보수 등 다양한 분야에 영향을 미치며, 나아가서는 시스템 전반에 영향을 미치게 된다. 또한 프로그램 에러의 대부분은 예상하지 못한 많은 입력 값에서 발생하며, 발생한 에러의 디버깅(Debugging)은 상대적으로 많은 인적, 물적 자원을 필요로 한다[4]. 그러므로 프로그램의 수행 중 발생한 에러에 대해 발생 위치를 추측, 추적하여 오류를 검출 하고 제어할 수 없거나 예상하지 못했던 오류의 발생 시 그 피해를 최소화 하며, 수정하기 쉽고 제품 코드에 손상을 덜 입히도록 만드는 것이 중요하다[2,4].

3. Adobe Flash Player의 보안 취약점에 대한 이공계 학부생의 인식도 조사

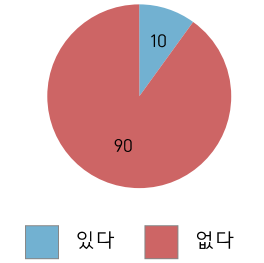
- 조사대상: 한국폴리텍대학 안성캠퍼스 학부생 100명
- 조사방법: 설문지를 통한 문답형 조사

3-1.Adobe Flash Player를 알고 있는가?

3-2.Adobe Flash Player를 자주 사용하는가?



3-3. Adobe Flash Player의 제로데이 보안 취약성을 알고 있는가?



- 조사결과: 설문조사 결과를 보면 대다수의 학생들이 Adobe Flash Player를 사용하며 알고 있었다. 하지만 보안문제를 느껴본 학생은 전체의 10%밖에 되지 않았다. 즉, Adobe Flash Player를 통해 학부생의 개인 정보가 유출 될 수 있음에도 불구하고 이를 인지하고 못하고 있었다.

4. 결론

오픈소스를 사용하는 것은 개발 과정에서 자신이 생각하지 못한 아이디어를 얻어 더 좋은 결과를 만들어 낼 수 있기 때문에 바람직하다. 하지만 편의성을 먼저 생각하여 보안문제를 등한시 한다면 완벽한 프로그램을 만들었다고 할 수 없다. 또한 출처가 불분명한 웹사이트 방문을 자제하여야 한다. 그리고 컴퓨터에 백신을 설치하여 보안 취약점과 관련된 악성코드를 수시로 검색하는 등과 같은 예방활동도 함께 수행되어야 한다.

참고문헌

[1] http://terms.naver.com/entry.nhn?docId=1228317
[2] Namuwiki(https://namu.wiki/w) - 보안강화
[3] https://tech.blorge.com/adobe-flash-player
[4] 오픈소스소프트웨어재단, “군과 OSS”, 2017
[5] https://www.dds.mil
[6] https://www.kisa.or.kr/main.jsp