오픈소스 보안 취약점 및 패치 현황 실시간 알림 시스템

최지은*, 구예림**, 전선진*** 박우인**** 이병희*****
*덕성여자대학교 컴퓨터공학과
**경기대학교 컴퓨터과학과
***숭실대학교 소프트웨어학부
****수원대학교 정보보호학과
*****네이버(주)
skskje312@naver.com, hoyu210@gmail.com, seonjinjeon.12@gmail.com, shionista@gmail.com, flittermouse@naver.com

OpenSource Security Vulnerability Real-Time Notification System

Ji Eun Choi*, Ye Lim Koo**, Seon Jin Jeon***, Woo In Park****, Byoung Hee Lee*****
* Dept. of Computer Engineering, Duksung Women's University
** Dept. of Computer Science, Kyonggi University
*** Dept. of Software, Soongsil University
**** Dept. of Information Security, Suwon University
*****Naver

요 약

기업 내에서는 다양한 오픈소스를 활용하고 있다. 이런 환경에서 해당 오픈소스의 취약점 및 패치 현황을 실시간으로 제공하여 빠르게 대처하는 것이 중요하다. 먼저 기업 내에서 많이 사용하는 오픈소스를 조사한 후 Top 70 오픈소스를 선정하여 보안 취약점 및 패치 현황을 파악한다. 실제 크롤링을 통해 취약점을 수집한 후, 필요한 정보를 가공하여 웹 서비스로 시각화 하여 제공한다. 또한 취약점이 발생했을 때 기업에서는 실시간 메일 알람 서비스를 받아볼 수 있는 과정을 제시한다.

1. 서론

1.1 개발 배경 및 필요성

IT 현업의 소프트웨어 엔지니어들은 다양한 오픈소스를 활용해 개발하고 있다. 이때 사용하는 오픈소스의 취약점 및 패치현황을 항상 모니터링할 수 없다는 현실적인 한계가 존재한다. 이러한 한계를 극복하기 위해 자주 사용되는 상위 70 개의 오픈소스의 취약점 및 패치 현황을 실시간으로 점검할 수 있는 어드바이저 프로그램 개발의 필요성이 있다. 따라서, 실시간으로 오픈소스의 보안 위협과 패치의 알람을 보낼 수 있는 자동화된 프로그램을 개발하여 IT 실무에 효율을 증진하고 낭비되는 시간과 비용을 최소화하고자 했다.

1.2 기존 서비스와의 차별점

기업 내에서 사용 빈도가 높은 오픈소스 파악 및 취약점을 확인할 수 있다. 실제 크롤링을 통해 필요한 정보를 시각화하여 제공할 수 있다. 또한, 등록해 놓은 이메일로 당일 오픈소스의 취약점 리스트를 전송 받을 수 있다.

2. 본론

2.1 시스템 개요

오픈소스를 활용해 개발이 진행되는 있는 상황에서 해당 오픈소스의 취약점 및 패치 현황을 실시간으로 제공하여 빠르게 대처하는 것이 중요하다. 따라서 본 프로젝트에서는 기업에서 자주 사용하는 오픈소스를 선정하여 보안 취약점 및 패치 현황을 실시간으로 확인할 수 있도록 한다.

2.2 기능 설계

사용자가 보안 취약점 및 패치 현황을 실시간으로 확인할 수 있도록 5 가지의 기능을 설계했다.

표 1 주요기능

기능	설명
크롤링	선별된 오픈소스 보안 패치 현황에 대한 크롤링
데이터 분석 및 가공	크롤링 데이터를 분석 및 가공하여 DB 저장

실시간 알람	오픈소스 보안 중요도에 따른 메일을 이용한 실시간 알림
데이터 시각화	오픈소스에 관한 CVE 통계 및 실시간 모니터링
데이터 번역	오픈소스 정보 영한번역

2.3 서비스 흐름도 설계

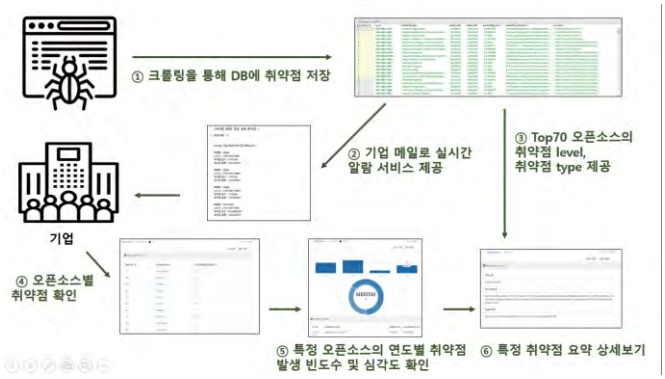


그림 1 동작 흐름도

3. 구현 결과

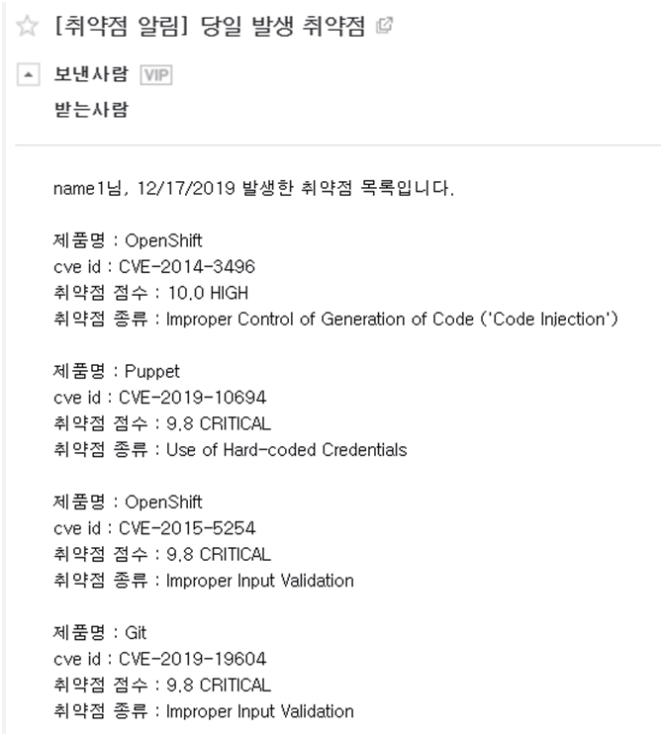
3.1 크롤링

CVE 취약점 사이트인 NVD 에서 오픈소스의 취약점을 크롤링하여 DB 에 저장했다. 해당 크롤링은 하루에 한번의 주기로 실행되어 데이터를 추출해 저장한다. 이 때, 기존에 확인된 취약점에 대해서는 다시 확인하지 않도록 설계하여 성능 측면의 리스크를 최소화 하였다.

그림 2 DB 에 저장된 취약점 리스트

3.2 실시간 알람

크롤링 데이터 중 당일 발생한 오픈소스의 취약점을 추출하여, 등록된 사용자의 이메일로 당일 오픈소스 취약점 리스트를 전송한다.



[취약점 알림] 당일 발생 취약점

보낸사람 VIP

받는사람

name1님, 12/17/2019 발생한 취약점 목록입니다.

제품명 : OpenShift
cve id : CVE-2014-3496
취약점 점수 : 10.0 HIGH
취약점 종류 : Improper Control of Generation of Code ('Code Injection')

제품명 : Puppet
cve id : CVE-2019-10694
취약점 점수 : 9.8 CRITICAL
취약점 종류 : Use of Hard-coded Credentials

제품명 : OpenShift
cve id : CVE-2015-5254
취약점 점수 : 9.8 CRITICAL
취약점 종류 : Improper Input Validation

제품명 : Git
cve id : CVE-2019-19604
취약점 점수 : 9.8 CRITICAL
취약점 종류 : Improper Input Validation

그림 3 메일로 전송된 오픈소스 취약점 실시간 알람

3.3 데이터 시각화

CVE 통계 및 실시간 모니터링을 위해 취약점 데이터를 시각화 한다. 시각화의 핵심은 직관적으로 알 수 있어야하고 위협 레벨에 따른 구분이 가능하도록 설계하였다.

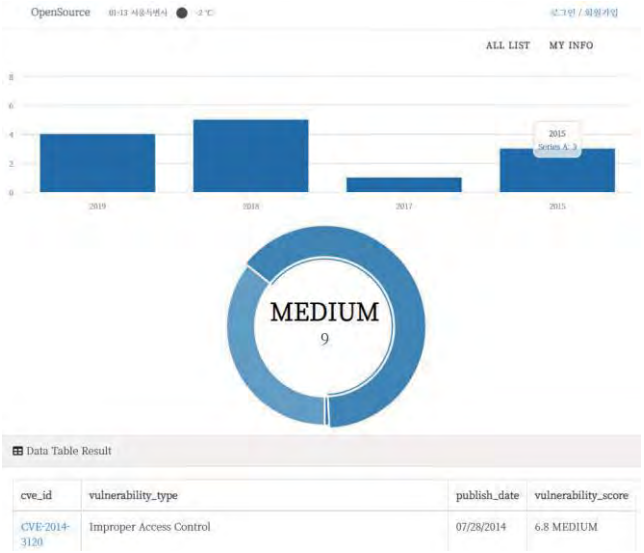


그림 4 오픈소스 취약점 데이터 시각화

4. 결론 및 향후 연구

최근 다양한 산학연에서 오픈소스의 활용이 증가하고 있다. 해당 시스템은 이러한 곳에서 오픈소스 취약점에 대한 실시간 알람을 통한 신속한 대응 가능할

것으로 기대된다. 또한, 최신 보안 취약점 경향 파악으로 오픈소스 활용에 대한 보안 위협 최소화에 도움을 줄 수 있을 것이다. 마지막으로 Threat Intelligence으로 보안 위협에 대한 자동화된 대응 체계 확립할 것을 기대한다.

향후 크롤링한 오픈소스 취약점 데이터의 심층 분석 및 위협 레벨에 대한 가공을 진행할 것이다. 번역 API 를 이용한 영한 번역을 통해 담당자가 쉽게 위협을 판단 할 수 있도록 확장할 예정이다. 또한 오픈소스의 확장을 통해 좀 더 많은 오픈소스 취약점을 실시간으로 탐지하고 반영할 수 있도록 할 것이다.

참고문헌

[1] 송석리, 이현아. “모두의 데이터 분석 with 파이썬”, 2019

[2] 사카타 코이치. “예제로 쉽게 배우는 스프링 프레임워크 3.0”, 2012

본 논문은 과학기술정보통신부

정보통신창의인재양성사업의 지원을 통해 수행한

ICT멘토링 프로젝트 결과물입니다.