

오픈소스 보안 취약점 관리 및 대응 전략

- 국방 사례 -

한컴MDS 국방사업실 김명호

2019.07.23



CONTENTS

I. 미 국방 오픈소스 관리 및 적용 사례

II. 한국 국방 오픈소스 관리 정책

III. 오픈소스 보안 취약점

IV. 오픈소스 보안 취약점 관리방안

Military Policy Governing OSS

- DoD Policy

- 2003 [OSS in the DoD \(Memo\)](#)
- 2006 [Open Technology Development Roadmap](#)
- 2009 [Clarifying Guidance Regarding Open Source](#)
- 2010 [Better Buying Power \(Memo\)](#)

: Open Architecture

- 국방 분야 소스 오픈, 오픈 소스 사용 권장, 오픈 아키텍처 등의 도입으로 비용 절감
- 소스코드 공개를 통해 발견하지 못한 코드의 취약점 발견
- 기타 지형, 모델링, 시뮬레이션 관련 분야 등 다양한 오픈소스 SW 개발 및 활용 중



DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

OCT 16 2009

CHIEF INFORMATION OFFICER

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
COMMANDERS OF THE COMBATANT COMMANDS
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES
CHIEF INFORMATION OFFICERS OF THE MILITARY DEPARTMENTS

SUBJECT: Clarifying Guidance Regarding Open Source Software (OSS)

References: See Attachment I

To effectively achieve its missions, the Department of Defense must develop and update its software-based capabilities faster than ever, to anticipate new threats and respond to continuously changing requirements. The use of Open Source Software (OSS) can provide advantages in this regard. This memorandum provides clarifying guidance on the use of OSS and supersedes the previous DoD CIO memorandum dated May 28, 2003 (reference (a)).

Open Source Software is software for which the human-readable source code is available for use, study, reuse, modification, enhancement, and redistribution by the users of that software. In other words, OSS is software for which the source code is "open."

[Clarifying Guidance Regarding Open Source](#)



OSS and DoD Policy

Q: What policies address the use of open-source software in the Department of Defense?

The following policies apply:

1. The DoD CIO issued a memorandum titled "[Clarifying Guidance Regarding Open Source Software \(OSS\)](#)" on 16 October 2009, which superseded a May 2003 memo from John Stenbit.
2. The Department of Navy CIO issued a memorandum with guidance on open source software on 5 Jun 2007. This memorandum only applies to Navy and Marine Corps commands, but may be a useful reference for others. This memo is available at <http://www.doncio.navy.mil/PolicyView.aspx?ID=312>.
3. The Open Technology Development Roadmap was released by the office of the Deputy Under Secretary of Defense for Advanced Systems and Concepts, on 7 Jun 2006. It is available at <http://www.acq.osd.mil/jctd/articles/OTDRoadmapFinal.pdf>.
4. The Office of Management and Budget issued a memorandum providing guidance on software acquisition which specifically addressed open source software on 1 Jul 2004. It may be found at <http://www.whitehouse.gov/omb/memoranda/fy04/m04-16.html>.
5. US Army Regulation 25-2, paragraph 4-6.h, provides guidance on software security controls that specifically addresses open source software. This regulation only applies to the US Army, but may be a useful reference for others. The regulation is available at http://www.army.mil/usapa/epubs/pdf/r25_2.pdf.

In nearly all cases, OSS is commercial software, so the policies regarding commercial software continue to apply to OSS.

General information about OSS

Q: Is open source software commercial software? Is it COTS?

Open source software that has at least one non-governmental use, and has been or is available to the public, is commercial software. If it is already available to the public and is used unchanged, it is usually COTS.

- OSS 사용에 대한 가이드 및 'The Open Technology Development Roadmap' 등을 공개하여 OSS의 사용을 권장하고 있음
- OSS를 상용 소프트웨어와 동일하게 취급하고 있으며 그에 따른 규정/법규 등을 따르도록 규정하고 있음



CHIEF INFORMATION OFFICER
U.S. DEPARTMENT OF DEFENSE



Q: Isn't using open source software forbidden by DoD Information Assurance Policy?

No. This misconception comes from a misinterpretation of DoD Instruction 8500.2, "Information Assurance (IA) Implementation", Enclosure 4, control DCPD-1.

The control in question reads:

DCPD-1 Public Domain Software Controls Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available. Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government.

This control is intended to limit the use of certain kinds of "binary or machine executable" software when "the Government does not have access to the original source code". As clarified in the 2009 DoD CIO Memorandum, this control does not prohibit the use of open source software, since with open source software the government *does* have access to the original source code.

In the [Desktop Application STIG version 3, release 1 \(09 March 2007\)](#); in its section 2.4, it clearly states that DCPD-1 does not apply to open source software, for this very reason. The STIG first notes that "DoD has clarified policy on the use of open source software to take advantage of the capabilities available in the Open Source community as long as certain prerequisites are met. DoD no longer requires that operating system software be obtained through a valid vendor channel and have a formal support path, if the source code for the operating system is publicly available for review". It notes in particular that three cases for software are acceptable:

1. A utility that has publicly available source code is acceptable.
2. A commercial product that incorporates open source software is acceptable because the commercial vendor provides a warranty.
3. Vendor supported open source software is acceptable.

The DISA STIG also notes "4. A utility that comes compiled and has no warranty is not acceptable." Thus, a program must come with either source code or a warranty; if it has neither, then special dispensation is required, since it difficult to review, repair, or extend the program either directly or via someone else.

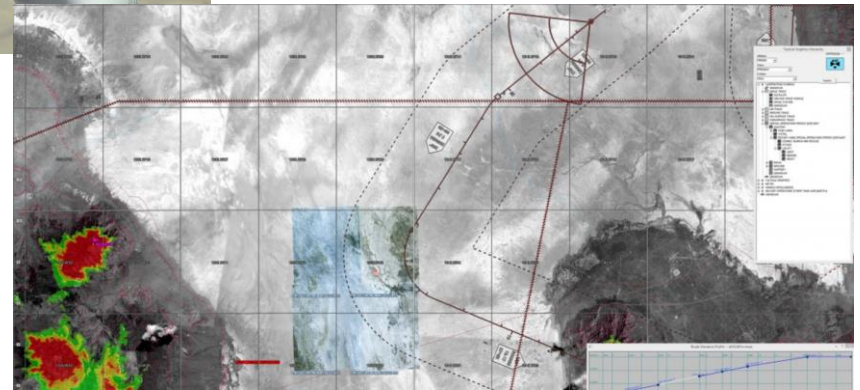
- Northrop Grumman 레이더 시스템의 OS를 윈도우에서 Linux로 변경
- Linux 기반의 소프트웨어로 모두 변경

Marines swap Microsoft for Linux OS on Northrop Grumman radar



해외 무기체계 오픈소스 적용 사례 (2/4)

- FalconView: 항공기 임무를 수행에 필수적인 지형 정보 지도로 장애물, 적소 위치 등의 정보를 제공



- DARPA 기타 사례



Examples of Open-Source Platforms



Source: Black-I Robotics

**LandShark
UGV**



Source: www.electronicshinfoline.com

**ArduPilot
UAV**



Source: Parrot
AR Drone

**AR Drone
UAV**

<http://resources.infosecinstitute.com/hack-proof-drones-possible-hacms-technology/#gref>

- 리눅스 적용 사례

- 9LV Mk4 (스웨덴, Saab 사 함정 전투체계)
- E-2C Hawkeye 2000 임무처리 (미국 Northrop Grumman, 조기경보기)
- TTWCS (Tomahawk 업그레이드) (미국, Lockheed martin, 미사일통제)
- RC-135 임무시스템 업그레이드 (미국, Boeing, 전투기 임무시스템)
- Aegis UYQ-70 콘솔 업그레이드 (미국, Lockheed Martin, 함정 전투체계)
- SSDS (미국, Raytheon, 함정 전투체계)
- TSCE DDS-1000 (미국, Raytheon, 함정 전투체계)
- 핵잠용 미해군 소나 시스템 (미국, Lockheed Martin, 핵잠수함 소나)
- AN/USG-2 (미국, 함정용)
- IPN-S (이탈리아, 함정 전투체계)
- ANCS2000 (독일, EADS, 함정 전투체계)
- SENIT2000 (프랑스, DCNS, 함정 전투체계)
- Sonar 2076 (영국, Thales, 잠수함용 소나 콘솔)
- SUBTICS (프랑스, UDS, 잠수함 전투체계)
- Battle control system (미국, Thales/Raytheon, 육군C4I)
- C-Flex (덴마크, Saab, 함정 전투체계)

CONTENTS

I. 미 국방 오픈소스 관리 및 적용 사례

II. 한국 국방 오픈 소스 관리 정책

III. 오픈소스 보안 취약점

IV. 오픈소스 보안 취약점 관리방안

무기체계 소프트웨어 개발 지원에 관한 규정

방위사업청 훈령 제327호(2015. 04. 09. 제정)
방위사업청 훈령 제377호(2016. 10. 17. 개정)
방위사업청 훈령 제471호(2018. 11. 28. 개정)

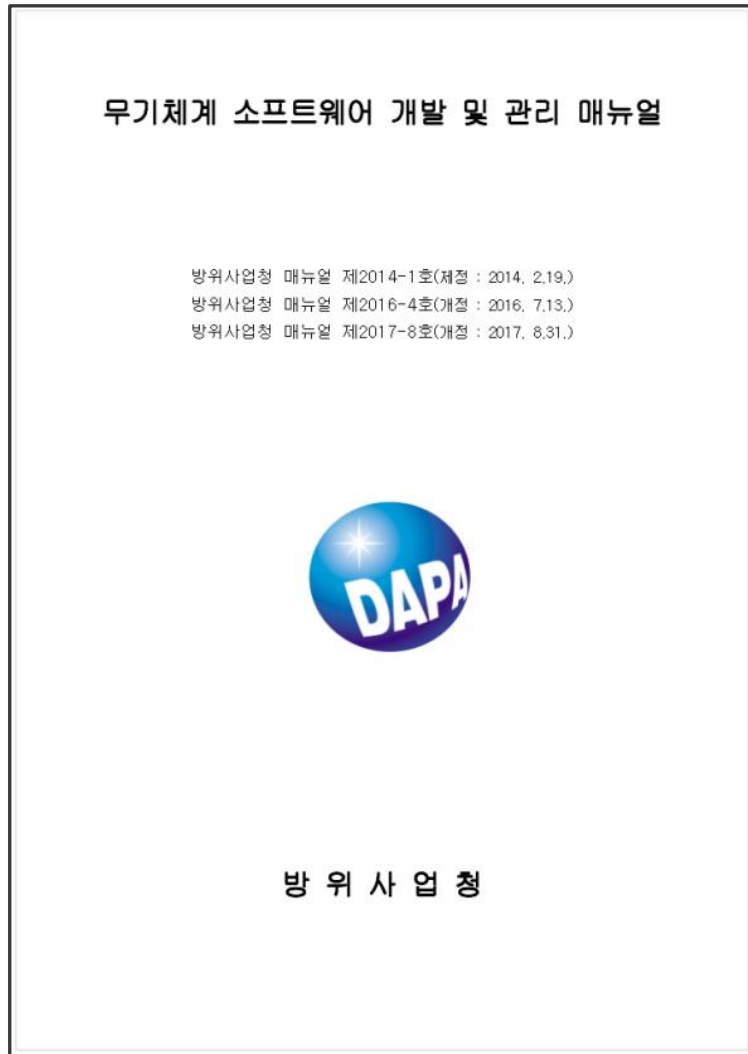


방 위 사 업 청

목 차

제3장 무기체계 소프트웨어 개발 기술지원

- 제10조(무기체계 소프트웨어 규격화)** ① 센터장은 통합사업관리팀장으로부터 기술지원을 요청받은 경우, 규격화 단계에서 소프트웨어의 최신 컴퓨터 파일(소스코드, 라이브러리, 실행파일, 데이터베이스 등) 및 관련 기술자료가 규격화되도록 기술지원을 실시하여야 한다.
- ② 제1항의 경우 통합사업관리팀장은 규격화에 필요한 소프트웨어 개발 산출물을 사전에 센터장에게 통보하여야 한다.
- ③ 센터장은 소프트웨어 소스코드의 신뢰성, 공개의무가 있는 소프트웨어 사용 여부, 최신 컴퓨터 파일(소스코드, 라이브러리, 실행파일, 데이터베이스 등) 및 기술자료 확인 등의 기술지원을 실시하고, 그 결과를 통합사업관리팀장에게 제출하여야 한다.
- ④ 기품원장은 방위사업관리규정 제123조 및 제602조에 따라 소프트웨어 규격화 자료에 대한 기술검토를 수행한다.



7. 지식재산권

...

라. 사업관리부서장은 소프트웨어 개발단계에서 소프트웨어 (공개 소프트웨어 포함)가 지식재산권 및 라이선스에 저촉되지 않도록 관리한다.

마. 연구개발주관기관은 연구개발 시 소스코드 공개 의무가 있는 공개 소프트웨어(Open Source)를 사용해서는 안된다.

【부록 7】소프트웨어 신뢰성/보안성 시험 절차

다. 적용 대상 소프트웨어

구 분	시험 대상여부
개발 소프트웨어	○
기개발 소프트웨어	×
상용(COTS) 소프트웨어 (HW와 함께 제공되는 SW 포함)	×
공개(Open) 소프트웨어	○
자동 생성 Code	○

2) 공개 소프트웨어는 부록14. 공개SW 무기체계 적용 가이드라인에 따라 소프트웨어 신뢰성 시험을 수행한다.

【부록 14】 공개SW 무기체계 적용 가이드라인

공개SW 무기체계 적용 가이드라인

부록 14 - 1

4. 적용 기준

가. 라이선스

- 1) 무기체계 연구개발 시 소스코드 공개 의무가 있는 공개SW를 사용해서는 안 된다. 단, 라이선스 구매 및 저작권자와 협의 등을 통해 소스코드를 공개하지 않아도 되는 것을 증명한 경우에는 사용 가능하다.

※ 공개SW인 운영체제 사용 필요 시 운영체제만을 공개 대상으로 하는 경우에 한하여 사업관리회의를 통하여 사용 여부를 결정한다.

- 2) 연구개발 주관기관은 공개SW 사용 시 특허권 등 권리 관계의 포함 여부를 사전에 확인하여 지식재산권 분쟁이 발생되지 않도록 관리하여야 한다.
- 3) SW에 관한 지식재산권과 공개SW 라이선스 의무사항을 준수한다.

나. 소프트웨어 신뢰성(정적, 동적) 시험

- 1) 상세설계 단계에서 공개SW의 사용 필요성과 신뢰성 확보 여부를 제시하고 사업관리회의에서 신뢰성이 확보된 공개SW로 판단된 경우 신뢰성 시험 대상에서 제외할 수 있다.

다. 소프트웨어 보안성 시험

- 1) 전장관리정보체계에 사용되는 공개SW에 대해서는 보안성 시험을 수행하는 것을 원칙으로 한다.

공개SW 사용 및 라이선스 준수여부 확인 목록

<< 공개SW 사용 목록 >>

번호	명칭	버전 (Release 식별 가능 정보)	라이선스	공개 의무 여부	특허 침해 여부	라이브러리/관련 소스 파일	비고 (출처 사이트 정보 및 캡처 화면)
1	OO SW	v1.0 (2014.04.02, 배포)	MIT	없음	없음	OO.dll OO.h	별첨 1
2	...	...	...	...	...	...	...
3	...	...	...	...	...	...	...
4							
...							

CONTENTS

I. 미 국방 오픈소스 관리 및 적용 사례

II. 한국 국방 오픈 소스 관리 정책

III. 오픈소스 보안 취약점

IV. 오픈소스 보안 취약점 관리방안



Heartbleed

OpenSSL 라이브러리에서 서버에 저장된 중요 메모리 데이터가 노출
(CVE-2014-0160)



ShellShock

GNU Bash에서 공격자가 원격에서 악의적인 시스템 명령을 실행 가능
(CVE-2014-6271)



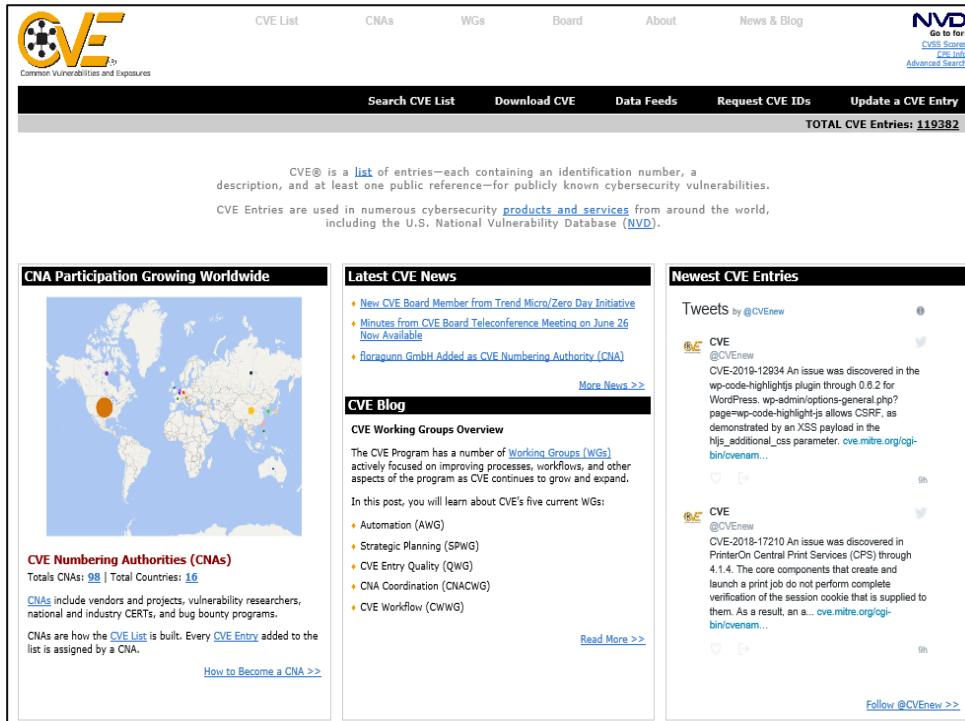
Drown

악성 패킷을 보내 인증서 키 값을 알아내고 이 키 값을 이용해
암호화된 통신 내용을 복호화 하여 주요 정보를 탈취하는
중간자 공격(Man-in-the-Middle attack)에 사용 가능
(CVE-2016-0800)



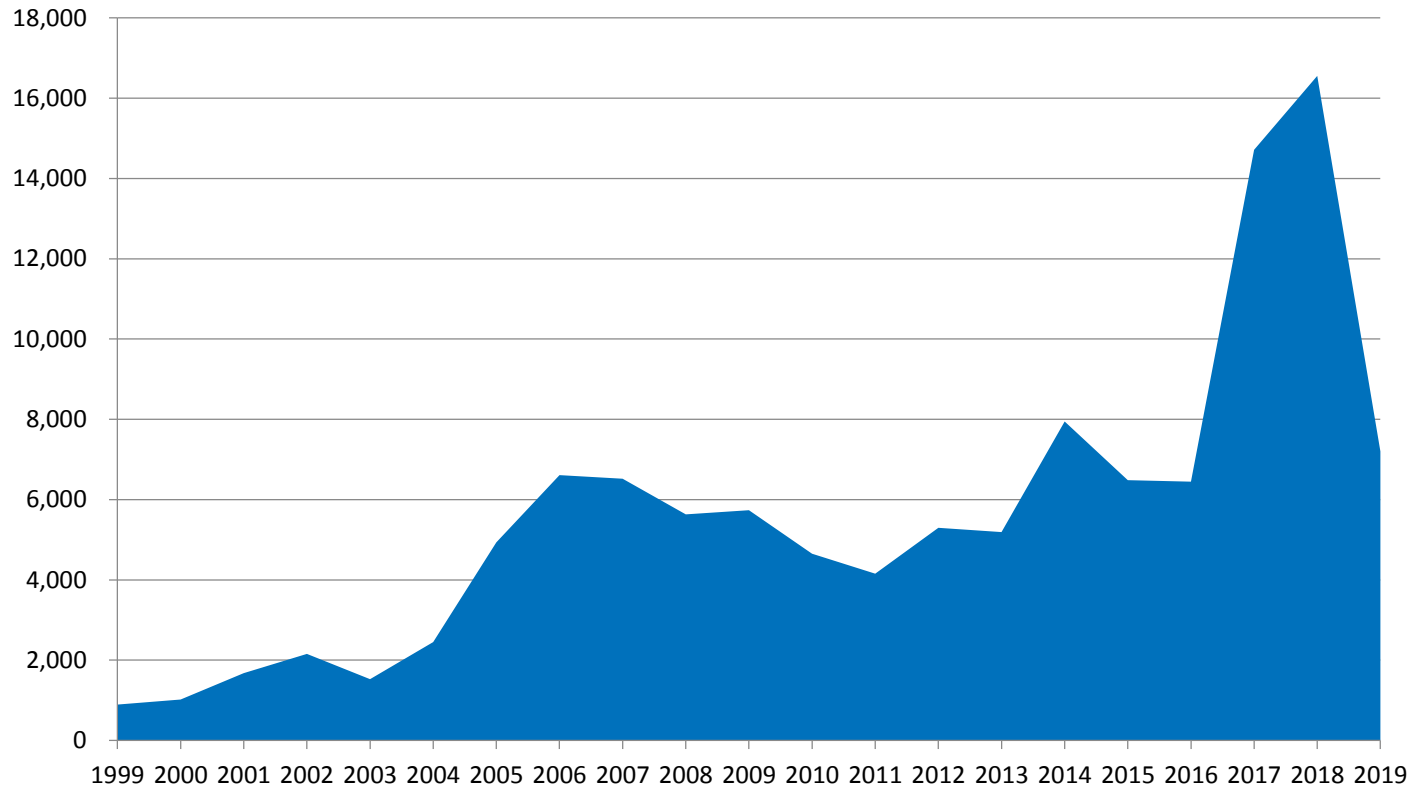
Ghost

GNU C 라이브러리(glibc)상의 원격코드 실행 취약점
리눅스 계열 시스템을 대상으로 원격에서 악성 파일을 실행하여
시스템을 임의로 조정하거나 저장된 데이터를 삭제 가능
(CVE-2015-0235)



- CVE : 사이버 보안 취약점에 대한 목록
- Each CVE Entry includes:
 - CVE ID [number](#) (i.e., "CVE-1999-0067")
 - Brief [Description](#) of the security vulnerability or exposure.
 - Any pertinent [References](#) (i.e., vulnerability reports and advisories).
- CNA(CVE Numbering Authority)
 - CVE ID를 할당 할 수 있는 기관
 - 대한민국: 한국인터넷진흥원, 네이버
- NVD(National Vulnerabilities Database)
 - NIST 에서 만든 국가 취약성 데이터베이스
 - CVE 목록을 기반으로 작성
 - 취약성 관리, 보안측정 및 컴플라이언스의 자동화에 기여

CVE의 신규 취약점 등록 수





- IT 취약성의 특성과 영향을 알려주는 **공개 프레임 워크**
- 국내외의 보안 전문기관 및 **실질적인 국제 표준**으로 사용
- 한국인터넷진흥원에서도 CVSS 기준으로 보안 취약점의 위험성을 표기

취약점의 주요 특징을 파악하고 수치 점수를 산출하는 방법을 제공
조직이 취약성 관리 프로세스를 적절하게 평가하고 우선 순위를 정할 수 있도록 수치 점수 제공

심각도	CVSS v3.0 Score Range	공격예시
Critical	9.0 ~ 10	루트 권한 원격코드 실행, 웜 등
High	7.0 ~ 8.9	권한상승 공격, 원격 DOS 등
Medium	4.0 ~ 6.9	로컬에서의 DOS, 웹사이트 디페이스, 인증이 필요한 공격
Low	0.1 ~ 3.9	공격난이도가 낮거나, 영향도가 낮은 경우

✓ Equifax 회사는 ?

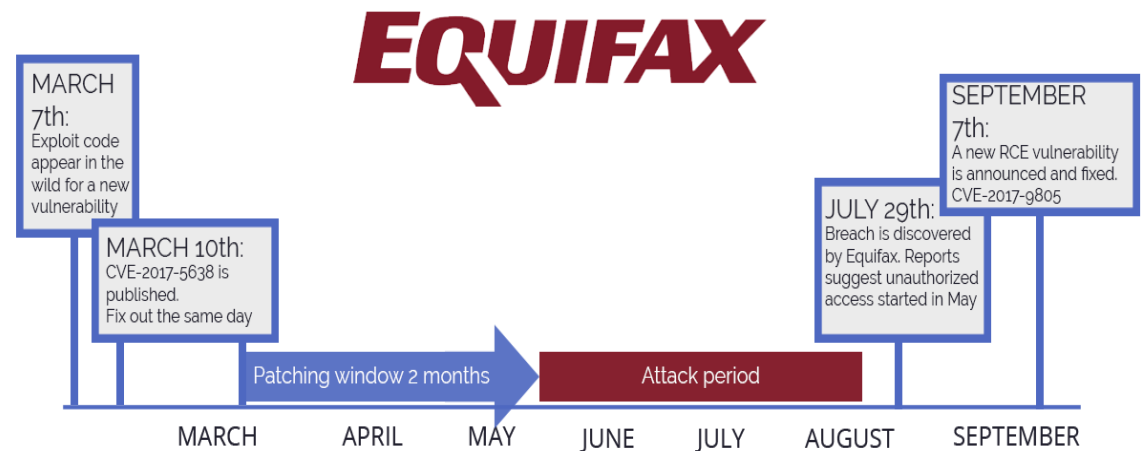
- ✓ 소비자 신용평가기관, 미국의 3대 신용회사 중 가장 오래된 회사
- ✓ 전 세계적으로 8억명이 넘는 개인 소비자와 88,000여 기업에 대한 정보 보유

✓ Equifax 보안 취약점을 이용한 개인정보 유출

- ✓ Equifax가 2달 간 무시했던 **Apache Struts** 취약점(CVE-2017-5638)을 이용한 공격
- ✓ 미국 전체인구의 절반 가량에 해당하는 1억 4,300만 명의 개인정보 유출
역사상 최대, 최악의 데이터 정보 유출 사건

✓ Equifax 보안 사고 여파

- ✓ Equifax 기업 이미지 실추
- ✓ 시가총액 약 40억 달러 하락
- ✓ CIO, CSO 사퇴에 이어 CEO 사퇴



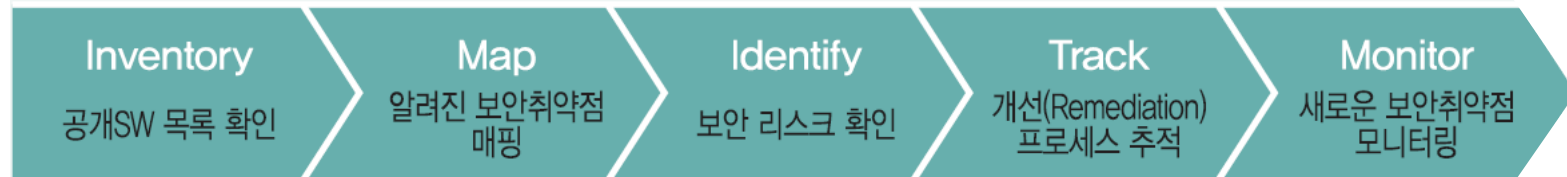
CONTENTS

I. 미 국방 오픈소스 관리 및 적용 사례

II. 한국 국방 오픈 소스 관리 정책

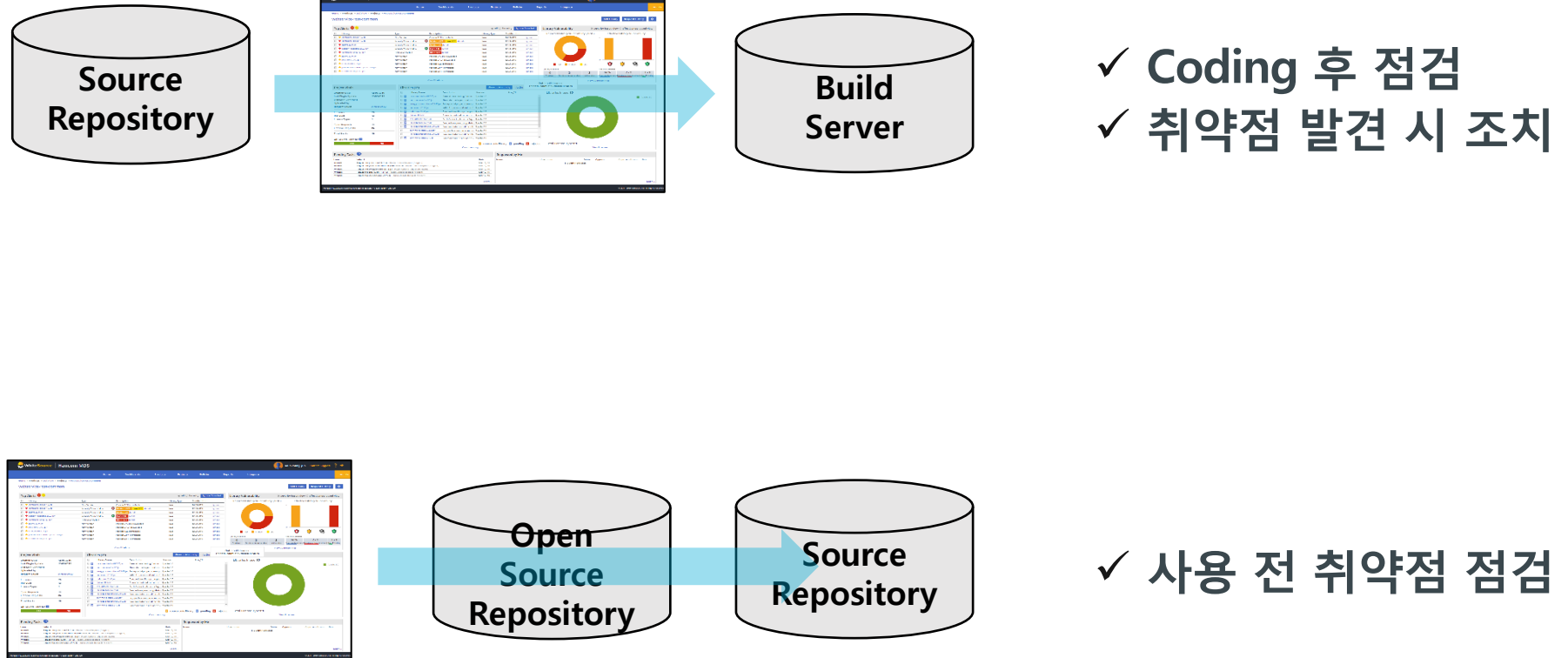
III. 오픈소스 보안 취약점

IV. 오픈소스 보안 취약점 관리방안



- 취약점을 찾고 패치를 적용할 부분을 알아내기 위해 프로젝트 내에 존재하는 공개SW 명칭과 버전확인
- 알아낸 명칭과 버전을 토대로 CVE 사전에서 취약점 검색
- 공개SW 목록과 검색한 보안취약점 매핑
- 해당되는 보안취약점으로 인한 보안 리스크 확인
- 패치유무 확인, 패치가능여부 확인, 패치적용 및 개선작업
- 새로운 보안취약점 파악을 위한 주기적인 모니터링

OSS Management System



오픈소스 취약점을 해결하기 위한 방법

 WhiteSource

Hancom MDS

 Mun Young. Juh

Contact Support

 →

HomeDashboardsProductsProjectsPoliciesReportsIntegrateAdmin

Home > Products > SoftFlow > Projects > webservice-rest-common

webservice-rest-common

Add LibraryRequest History

Top Alerts416

AllSecurityIgnore Selected

Library	Type	Description	Library Type	Modified Date	
☐ commons-codec-1.5.jar	New Version	Version 1.11 is available	Java	14-03-2019	ignore
☐ commons-codec-1.5.jar	Security Vulnerability	Medium: 1 (1) Low: 1 (0) details	Java	12-03-2019	ignore
☐ guava-20.0.jar	Security Vulnerability	Medium: 1 details	Java	12-03-2019	ignore
☐ jackson-databind-2.9.7.jar	Security Vulnerability	High: 1 (0) details	Java	12-03-2019	ignore
☐ commons-lang3-3.1.jar	High Severity Bug	Blocker: 1 details	Java	12-03-2019	ignore
☐ guava-20.0.jar	New Version	Version 27.0-jre is available	Java	12-03-2019	ignore
☐ joda-time-2.9.2.jar	New Version	Version 2.10.1 is available	Java	12-03-2019	ignore
☐ snakeyaml-1.17.jar	New Version	Version 1.23 is available	Java	12-03-2019	ignore
☐ jackson-dataformat-yaml-2.8.5.jar	New Version	Version 2.9.7 is available	Java	12-03-2019	ignore
☐ commons-lang3-3.1.jar	New Version	Version 3.8.1 is available	Java	12-03-2019	ignore

View All Alerts

Project Vitals

Creation Date12-03-2019

Last Plugin Update12-03-2019

Last Scan Comment

Uploaded by

Request Tokenclick to copy

Libraries15

In-House13

License Types1

Open Requests13

Lifetime Requests26

Total Alerts10

Up-To-Date Libraries?YesNo

Libraries (15)

Show as HierarchyAction

Library Name	Description	Licenses	Attr_01
☐ jackson-databind-2.9.7.jar	General data-binding functio...	Apache 2.0	
☐ commons-codec-1.5.jar	The codec package contains s...	Apache 2.0	
☐ swagger-annotations-1.5.13.jar	Sonatype helps open source p...	Apache 2.0	
☐ snakeyaml-1.17.jar	YAML 1.1 parser and emitter f...	Apache 2.0	
☐ joda-time-2.9.2.jar	Date and time library to repla...	Apache 2.0	
☐ guava-20.0.jar	Guava is a suite of core and e...	Apache 2.0	
☐ evo-inflector-1.2.1.jar	Evo Inflector implements Engl...	Apache 2.0	
☐ jackson-core-2.9.7.jar	Core Jackson processing abstr...	Apache 2.0	
☐ jackson-annotations-2.9.0.jar	Core annotations used for val...	Apache 2.0	
☐ commons-lang3-3.2.1.jar	org.apache.commons:commo...	Apache 2.0	
☐ jackson-annotations-2.8.5.jar	Core annotations used for val...	Apache 2.0	
☐ commons-lang3-3.1.jar	Commons Lang: a package of ...	Apache 2.0	

View Inventory

S - source code library P - pending R - rejected

Outdated Libraries:

The total count of outdated libraries

Libraries in use: 15

Apache 2.0

Total License Types: 1

View Licenses

Library Vulnerability

Severity-based ViewEffectiveness-based View

Reported Library Vulnerability (HIGH)

Effective Library Vulnerability

Library Statistics

Analysis Statistics

View Vulnerabilities

Pending Tasks13

From	Subject	Date
Kwansik	Request for joda-time-2.9.2.jar - Plugin Update Request (fs-agent)	Mar 12, 19
Kwansik	Request for jackson-dataformat-yaml-2.8.5.jar - Plugin Update Request (fs-agent)	Mar 12, 19
Kwansik	Request for swagger-core-1.5.13.jar - Plugin Update Request (fs-agent)	Mar 12, 19
Kwansik	Request for snakeyaml-1.17.jar - Plugin Update Request (fs-agent)	Mar 12, 19
Kwansik	Request for jackson-core-2.9.7.jar - Plugin Update Request (fs-agent)	Mar 12, 19

More...

Requested by Me

Name	Description	Status	Approver	Approvers Group	Date
No Sent Requests					

More...

Version 19.2.2.60 | Last vulnerabilities update: 18-Mar-2019, 12:00 AM

© 2011-2019 WhiteSource. All rights reserved

오픈소스 취약점을 해결하기 위한 방법

 WhiteSource

Hancom MDS

Home

Dashboards

Products

Projects

Policies

Reports

Integrate

Admin

Home > Products > SoftFlow > Projects > webservice-rest-common

webservice-rest-common

Top Alerts 4 10

Library

commons-codec-1.10.0.jar

commons-codec-1.10.0.jar

guava-20.0.jar

jackson-databind-2.9.8.jar

commons-lang3-3.9.jar

guava-20.0.jar

joda-time-2.9.2.jar

snakeyaml-1.17.jar

jackson-dataformat-yaml-2.9.8.jar

commons-lang3-3.9.jar

Project Vitals

Creation Date

Last Plugin Update

Last Scan Comment

Uploaded by

Request Token

Libraries

In-House

License Types

Open Requests

Lifetime Requests

Total Alerts

Up-To-Date Libraries 100%

Yes

Pending Tasks 13

From

Subj

Kwansik

Req

Kwansik

Req

Kwansik

Req

Kwansik

Req

Kwansik

Req

WhiteSource

Hancom MDS

Home

Dashboards

Products

Projects

Policies

Reports

Integrate

Admin

Home > Dashboards > Release Management

Release Management

Product - PROD

Export to HTML

License Text

AGPL

Apache 1.1

Apache 2.0

BSD

BSD 3

Bouncy Castle License

CC BY 2.5

CC BY 3.0

CC BY SA 3.0

CC0 1.0

Licenses with no text file

Suspected Apache 2.0

Suspected CDDL 1.1

Suspected Commercial

Suspected GPL 3.0

Suspected LGPL 3.0

Suspected Public Domain

Suspected Unspecified License

Libraries with unknown license: 48

To view and handle go to Product

Notices and Copyrights

Notice	Copyright	Library	Actions
☐	X	X	select2-3.4.5.js
☐	X	✓	cdi-api-1.0.jar
☐	X	X	tomcat-118n-ja-8.0.53.jar
☐	X	✓	xmlbeans-2.6.0.jar
☐	X	✓	netcdf-4.2.20.jar
☐	X	X	canvas-to-blob-3.12.0.min.js
☐	X	X	mariaadb-java-client-1.1.8.jar
☐	X	X	hone-integration-4.0.0-SNAPSHOT.jar
☐	X	✓	ant-launcher-1.9.4.jar
☐	X	✓	commons-discovery-0.2.jar
☐	X	X	tomcat-jni-8.0.53.jar
☐	X	✓	jfreechart-1.0.19.jar
☐	X	X	tomcat-catalina-ha-8.0.53.jar
☐	X	✓	jmatio-1.0.jar
☐	X	X	logstash-core.jar
☐	X	X	hone-pci-4.0.0-SNAPSHOT.jar
☐	X	X	jquery.flot.resize-0.7.0.js
☐	X	X	logstash-codec-json-v3.0.5
☐	X	X	jsr250-api-1.0.jar
☐	X	✓	commons-codec-1.9.jar

Download Notices File

Download Copyrights File

Help

Licenses

Download a zip file containing all license text files of licenses from your product.

Licenses with no text file will not be included in the zip file.

Notices

Generate a single notice text file for all relevant library notices.

You must make sure that notices are present when necessary. The "Notice" column indicates when the library has a notice.

You may add notices by clicking the "set notice" link or by using the suggestion.

If you do not wish to include a library in the notice file, click the "hide" link.

Version 18.12.2 | Last vulnerabilities update: 15-Jan-2019, 12:00 AM

© 2011-2019 WhiteSource. All rights reserved

Version 19.2.2.2.60 | Last vulnerabilities update: 18-Mar-2019, 12:00 AM

 HANCOM

한컴MDS

오픈소스 취약점을 해결하기 위한 방법

 WhiteSource | Hancom MDS

 Donghyun Nam

Contact Support ? →

HomeDashboardsProductsProjectsPoliciesReportsIntegrateAdmin

Home > Security Vulnerability (CVE-2017-12626)

Security Vulnerability

General Details

Name	Severity	CVSS 3 Score	CVSS 2 Score	Date	Modified
CVE-2017-12626	High	7.5	5.0	30-01-2018	05-05-2018

Apache POI in versions prior to release 3.17 are vulnerable to Denial of Service Attacks: 1) Infinite Loops while parsing crafted WMF, EMF, MSG and macros (POI bugs 61338 and 61294), and 2) Out of Memory Exceptions while parsing crafted DOC, PPT and XLS (POI bugs 52372 and 61295).

CVSS 3 - Base Score Metrics

Exploitability Metrics

Attack Vector (AV) ?
NETWORK

Attack Complexity (AC) ?
LOW

Privileges Required (PR) ?
NONE

Impact Metrics

Confidentiality Impact (C) ?
NONE

Integrity Impact (I) ?
NONE

Availability Impact (A) ?
HIGH

Vulnerable Libraries

Library Name
poi-scratchpad-3.11-beta2.jar

Total: 1

Vulnerabilities (28)

Severity	Library	Vulnerability Id	Score	Description (hover for full t
High	spring-webmvc-3.2...	CVE-2016-9878	7.5	An issue was discovered in Piv
High	poi-scratchpad-3.11...	CVE-2017-12626	7.5	Apache POI in versions prior t
High	xercesimpl-2.8.1.jar	CVE-2013-4002	7.1	XMLScanner.java in Apache X

Fixes (1)

Show References

★

Change Files

Replace or update the following files: HwmfPicture.java, TestHwmfParsing.java, 61338.wmf

Commit a07ed9e: 61338 -- avoid infinite loop triggered by fuzzed wmf file git-svn-id: https://svn.apache.org/repos/asf/poi/trunk@1802997 13f79535-47bb-0310-9956-ffa450edef68

Vulnerability DB Links

Common Vulnerabilities and Exposures (CVE)

National Vulnerability Database (NVD)

Version 18.12.2 | Last vulnerabilities update: 15-Jan-2019, 12:00 AM

© 2011-2019 WhiteSource. All rights reserved.

오픈소스 취약점을 해결하기 위한 방법

Home > Library Security Vulnerabilities

poi-scratchpad-3.11-beta2.jar

Product PROD Project TMOVER Apply Preferred

Security Vulnerabilities (2)

Export

Severity	Vulnerability Id	CVSS 3 Score	CVSS 2 Score	Description (hover for full text)	Published	Top Fix
High	CVE-2017-12626	7.5	5.0	Apache POI in versions prior to release 3.17 are vulnerable to Denial of Service Attacks: 1) Infinite Loops while parsing crafted WMF, EMF, MSG and macros (POI bugs 61338 and 61294), and 2) Out of Memory Exceptions while parsing crafted DOC, PPT and XLS (POI bugs 62372 and 61295).	30-01-2018	Replace or update the following files: HwmfPicture.java, TestHwmfParsing.java, 61338.wmf The reported vulnerability was not checked for vulnerability effectiveness and is suggested to be examined using Effective Usage Analysis.
Medium	CVE-2014-9527	-	5.0	HSLFSlideShow in Apache POI before 3.11 allows remote attackers to cause a denial of service (infinite loop and deadlock) via a crafted PPT file.	07-01-2015	Replace or update the following files: TestBugs.java, HSLFSlideShow.java, 57272_corrupted_usereditatom.ppt The reported vulnerability was not checked for vulnerability effectiveness and is suggested to be examined using Effective Usage Analysis.

"WS" vulnerabilities were verified by the WhiteSource security research team

"CVE" vulnerabilities were verified by NVD



Top Alerts 12 11		
Library	Type	Description
☐ spring-core-3.2.3.RELEASE.jar	Security Vulnerability	Medium: 1 details
☐ spring-web-3.2.3.RC1.FAS.jar	Security Vulnerability	High: 2 Medium: 4 details
☐ poi-scratchpad-3.11-beta2.jar	Security Vulnerability	High: 1 Medium: 1 details
☐ poi-ooxml-3.9.jar	Security Vulnerability	Medium: 3 details
☐ xercesImpl-2.8.1.jar	Security Vulnerability	High: 1 Medium: 1 details
☐ spring-webmvc-3.2.3.RELEASE.jar	Security Vulnerability	High: 3 Medium: 2 details
☐ spring-ldap-core-1.3.2.RELEASE.jar	Security Vulnerability	High: 1 details
☐ spring-security-config-3.2.3.RELEASE.jar	Security Vulnerability	High: 1 details
☐ bcprov-jdk15-1.45.jar	Security Vulnerability	Medium: 1 details
☐ spring-security-web-3.2.3.RELEASE.jar	Security Vulnerability	High: 2 details

오픈소스 취약점을 해결하기 위한 방법

 WhiteSource | Hancom MDS

 Mun Young, Juh [Contact Support](#) [?](#) [→](#)

[Home](#) [Dashboards](#) [Products](#) [Projects](#) [Policies](#) [Reports](#) [Integrate](#) [Admin](#)

[Home](#) > [Hancom MDS](#) > [Policies](#) > Add policy

Add Policy

Name

New Policy

Match

By License Group

Licenses

☐ License Name

☐ Apache 1.0

☐ Apache 1.1

☐ Inclusive (trigger only when ALL licenses of the Library are matched)

Remove Selected

Add Licenses

Action

☐ Approve

☒ Reject

☐ Reassign

☐ Conditions

☐ Issue

Approve(화이트리스트) - 라이브러리에 대한 자동 허용

Reject (블랙리스트) - 라이브러리에 대한 자동 거부

Reassign - 지정된 사용자에게 분석 요청을 재 할당

Conditions - 정책 적용 기간 등의 조건 지정

Issue - Jira등의 이슈 관리 시스템과 연동

Add

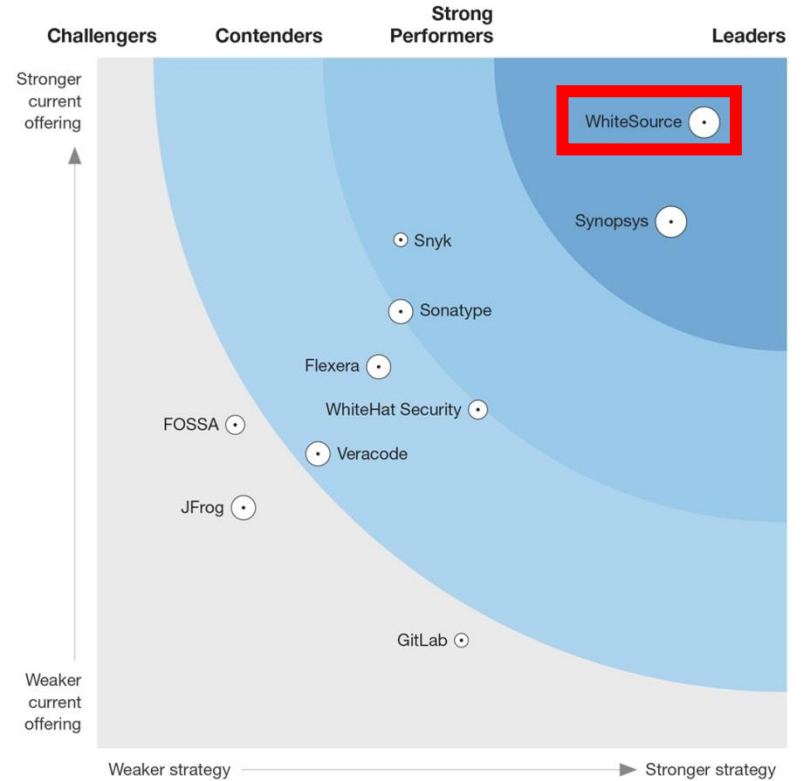
Cancel

Version 19.1.2.44 | Last vulnerabilities update: 20-Feb-2019, 06:00 AM

© 2011-2019 WhiteSource. All rights reserved

THE LEADER OF SOFTWARE COMPOSITION ANALYSIS

The Forrester Wave™ Q2 2019



Founded in 2011.
Offices in NY, Boston,
London & Tel-Aviv



900+
Customers



Empowering over
1.2 M
developers



Supporting **30%+**
of Fortune 100
companies



Over **3x**
YOY growth



COMPLETENESS

- 200개 이상의 지원
- 20여 개 바이너리 분석 지원
- 모든 개발환경에서 활용 가능한 완벽한 솔루션



PRIORITIZATION

- 종합적인 오픈 소스 위험 평가
- 취약점 우선 순위 선택
- 디지털 시그니처 분석 방식으로 오탐 (False Positive) 방지



REMEDiation

- 실시간 취약점 탐지 및 업데이트 되는 취약점 자동 알림
- 취약점 별 해결방안 제공

- ✓ OSS 사용은 반드시 필요
- ✓ 예방적 OSS 관리 체계 (제도, Process, IT System 등) 구축 검토
- ✓ 지속적 개발자 교육 및 사내 OSS 전문가 양성

Q & A

인텔리전트 융합 솔루션 전문기업

(주)한컴MDS

(주)한컴MDS www.hancommds.com

본사 13493 경기도 성남시 분당구 대왕판교로 644번길 49 한컴타워 3,4층 031-627-3000

연구소 13487 경기도 성남시 분당구 판교로 228번길 17 판교세븐벤처밸리 2단지 1동 9층 031-600-5000