

FOSSLight Hub로 보안취약점 관리해요

2023. 06. 22

LG전자 석지영



FOSSLight Hub

FOSSLight Hub

오픈소스 및 라이선스 관리



- 오픈소스 정보 통합 관리
- 라이선스 의무사항 및 제약사항 확인
- 오픈소스 일괄 등록

컴플라이언스 프로세스 관리



- 올인원 오픈소스 컴플라이언스 수행
- 고지문 자동 생성 및 공개 소스코드 검증
- 이슈 트래킹

보안취약점 관리



- 보안취약점 조회
- 프로젝트별 보안취약점 모니터링 (자동 메일 알림)

사전점검



- 오픈소스 자동 분석
- 라이선스 자동 검출
- 라이선스 의무사항 및 보안취약점 알림

SBOM 관리



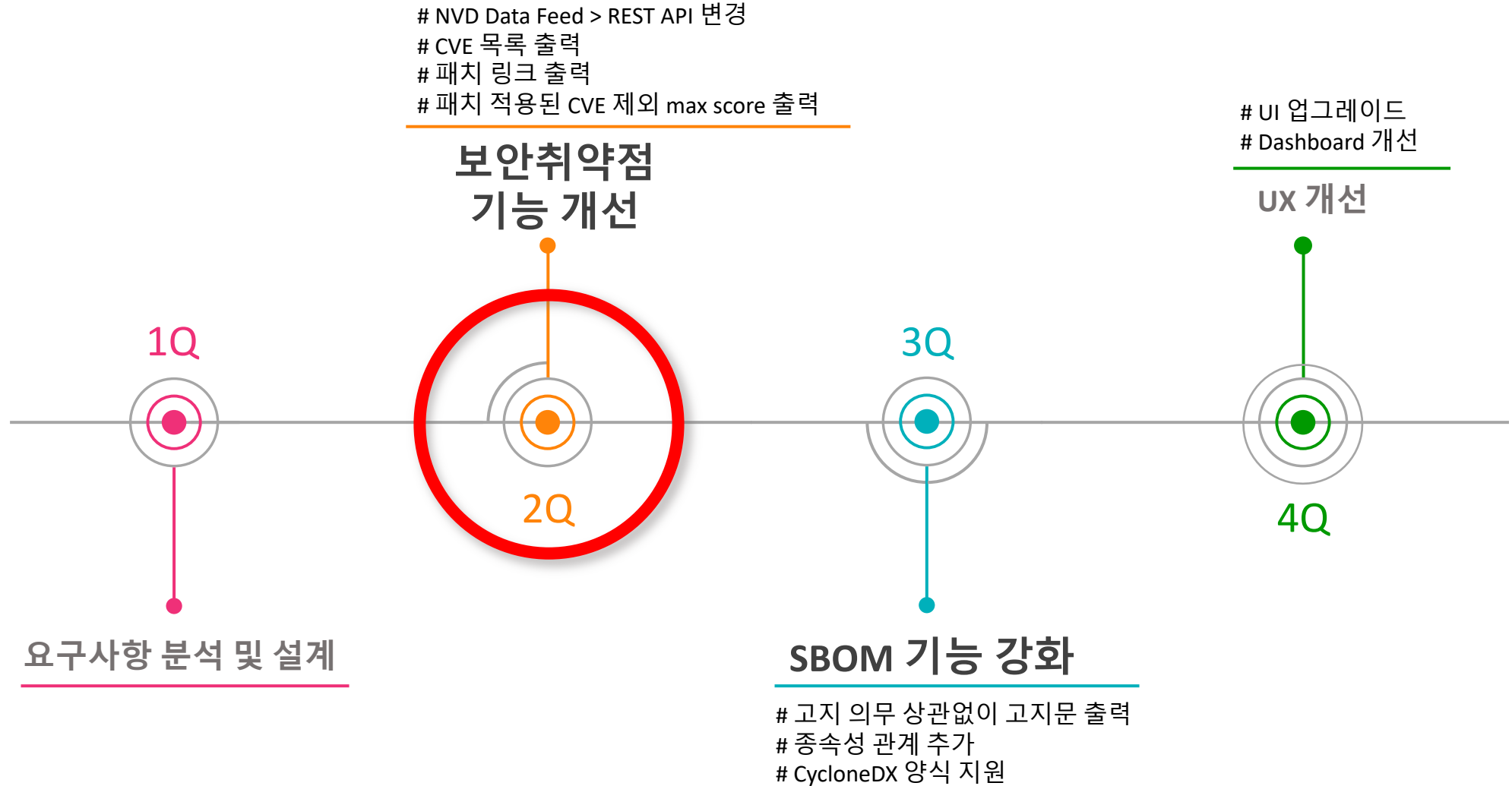
- 오픈소스 및 상용 소프트웨어 목록 관리
- 소프트웨어별 사용 프로젝트 검색
- SPDX 문서 지원 (ISO 표준)

공급망 관리



- 공급받은 타사 소프트웨어 관리
- 오픈 소스 확약서 관리
- 프로젝트 자동 연계

FOSSLight Hub 2023 업데이트 일정



NVD REST API 변경

NVD REST API 변경

- ❑ Vulnerability 정보는 매일 NVD Rest API (2.0 API)를 통해 Data 취합하여 업데이트
- ❑ Vulnerability Score는 CVSS v3 Base Score 기준으로 표기
(v3 Score가 없는 경우 CVSS v2 Base Score 대신 표기)



VULNERABILITIES

NVD Data Feeds

NOTICE

In September 2023, the NVD plans to retire all legacy data feeds while guiding any remaining data feed users to updated application-programming interfaces (APIs). APIs have many benefits over data feeds and have been the proven and preferred approach to web-based automation for over a decade. For additional information on the NVD API, please visit the [developers pages](#). [Click here](#) for more information on the NVD timeline.

보안취약점 조회 (Vulnerability 메뉴)

□ Open Source 보안 취약점 존재 여부 및 관련 정보(CVE ID, CVSS Score) 확인

The screenshot shows the FOSSLight interface with the 'Vulnerability' menu selected. The search filters are set to 'OSS Name: spring framework' and 'CVE ID: CVE-****_*'. The search results list shows multiple entries for 'spring_framework' with various versions and CVE IDs. A detailed view of a vulnerability is shown in a pop-up window, listing the following data:

OSS Name	Version	Score	CVE ID	Modified Date
spring_framework	2.5.0	7.5	CVE-2011-2730	2017-08-09
spring_framework	2.5.0	6.0	CVE-2010-1622	2023-02-13
spring_framework	2.5.0	5.0	CVE-2009-1190	2018-10-30

The detailed view also shows a table of versions with their respective scores and vendor information:

Version	Score	Vendor
2.1	7.5	springsource
2.5.0	7.5	springsource
2.5.1	7.5	springsource
2.5.2	7.5	springsource
2.5.3	7.5	springsource
2.5.4	7.5	springsource

보안취약점 조회 (Identification)

488_Identify

Project | hr-Training Project (1.1) B P | Creator | Admin SW Lab (2023-04-06)

3rd party | SRC | BIN | **BOM** | Reject

Show Comment History Comment Edit


OSS bulk registration

Export Yaml

ID	ReferenceD	OSS Name	OSS Version	License	Download Location	Homepage	Copyright Text	Vulnerability	Obligation		Restriction	admin check
									Notify	Source		
		~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	>= <input type="text"/> x				
1	BIN	pm2	3.5.2	AGPL-3.0	https://www.npmjs.com	https://www.npmjs.com	Copyright (c) 2013 the PM2 project Copyr				R	<input type="checkbox"/>
1	3rd	Apache Ant	1.6.5	Apache-2.0	http://archive.apache.org	http://ant.apache.org						<input type="checkbox"/>
2	3rd	Linux Kernel	2.6.28	GPL-2.0	https://www.kernel.org/	https://www.kernel.org/	copyright (C) 1997-2014 by The Linux Ke					<input type="checkbox"/>
3	3rd	Microsoft-tslib	1.9.0	Apache-2.0	https://github.com/Microsoft	https://www.npmjs.com	Copyright (c) Microsoft Corporation.					<input type="checkbox"/>
2	BIN	askalono		Apache-2.0	https://github.com/jpeddie	https://github.com/jpeddie	Copyright (c) 2018 Amazon.com, Inc. or i					<input type="checkbox"/>
1	SRC	caniuse-lite	1.0.30001037	CC-BY-4.0	https://www.npmjs.com	https://www.npmjs.com						<input type="checkbox"/>
3	BIN	error_prone_annotations	2.7.1	Apache-2.0	https://mvnrepository.com	https://mvnrepos	Copyright (c) 2015-2017 The Error Prone					<input type="checkbox"/>
24	SRC	httptools	0.1.1	MIT	https://pypi.org/project/	https://github.com	Copyright (c) 2015 MagicStack Inc. http://					<input type="checkbox"/>
31	SRC	log4j	1.2.8	Apache-1.1	http://archive.apache.org	http://logging.ap	Copyright (c) 2000-2002 Apache Software					<input type="checkbox"/>
4	3rd	pulseaudio	10.99.1	LGPL-2.1,GPL-2.0	https://freedesktop.org/	http://www.pulse	Copyright 2004-2006 Lennart Poettering C					<input type="checkbox"/>


Release Security tab

FOSSLight Hub




오픈소스 및 라이선스 관리

- 오픈소스 정보 통합 관리
- 라이선스 의무사항 및 제약사항 확인
- 오픈소스 일괄 등록




컴플라이언스 프로세스 관리

- 올인원 오픈소스 컴플라이언스 수행
- 고지문 자동 생성 및 공개 소스코드 검증
- 이슈 트래킹




보안취약점 관리

- 보안취약점 조회
- 프로젝트별 보안취약점 모니터링 (자동 메일 알림)
- 프로젝트별 보안취약점 해결 여부 관리




사전점검

- 오픈소스 자동 분석
- 라이선스 자동 검출
- 라이선스 의무사항 및 보안취약점 알림



SBOM 관리

- 오픈소스 및 상용 소프트웨어 목록 관리
- 소프트웨어별 사용 프로젝트 검색
- SPDX 문서 지원 (ISO 표준)



공급망 관리

- 공급받은 타사 소프트웨어 관리
- 오픈 소스 확약서 관리
- 프로젝트 자동 연계

Security 탭

□ 프로젝트 별 사용된 오픈 소스의 보안취약점 목록을 CVE ID별로 확인 가능

ID	Project Name (Version)	Status	Identification	Packaging	Download	Security	Vulnerability	Distribution Type	Division	Creator	Created Date	Updated Date	Reviewer	Additional Information
499	newOne	P	Start					General Model	SW Lab	Admin	2023-05-08	2023-05-08		
498	mytestproject12345	P	Confirm 3rd SRC BIN BOM	Start		SEC	▲	General Model	SW Lab	Admin	2023-05-03	2023-05-03	Admin	
497	cdh_test	R	Confirm 3rd SRC BIN BOM	Confirm		SEC	▲	General Model	SW Lab	Admin	2023-04-25	2023-04-25	Admin	
496	bxxt	P	Progress 3rd SRC BIN BOM			SEC		General Model	SW Lab	사용자	2023-04-21	2023-04-21		

□ Security 탭

Total
Fixed
Not Fixed

Show Comment History
Comment Edit

Export
Save

OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerability Link
Protocol Buffers		CVE-2015-5237	8.8	2017-09-25	Unresolved	https://nvd.nist.gov/vuln/detail/
Protocol Buffers		CVE-2021-3121	8.6	2021-01-11	Unresolved	https://nvd.nist.gov/vuln/detail/
SnakeYAML	1.27	CVE-2022-1471	9.8	2022-12-01	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	5.3.1	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	5.3.1	CVE-2022-22965	9.8	2022-04-01	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	4.3.30	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/

Security탭 – CVE 정보

☐ CVE ID별 NVD API 통해 해당 정보 출력

- CVSS Score, Published Date, NVD URL

OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerability Link
Protocol Buffers		CVE-2015-5237	8.8	2017-09-25	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2015-5237
Protocol Buffers		CVE-2021-3121	8.6	2021-01-11	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2021-3121
SnakeYAML	1.27	CVE-2022-1471	9.8	2022-12-01	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2022-1471
Spring Framework	5.3.1	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2016-1000027
Spring Framework	5.3.1	CVE-2022-22965	9.8	2022-04-01	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2022-22965
Spring Framework	4.3.30	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2016-1000027
Spring Framework	4.3.30	CVE-2022-22965	9.8	2022-04-01	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2022-22965
Spring Framework	4.3.19	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2016-1000027
Spring Framework	4.3.19	CVE-2022-22965	9.8	2022-04-01	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2022-22965
hazelcast	5.1	CVE-2022-0265	9.8	2022-03-03	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2022-0265

Security탭 – Vulnerability Resolution

□ Vulnerability Resolution

- 수정 여부에 따라 Resolution값 선택 가능

OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerability Link
~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>	x ~ <input type="text"/>
Protocol Buffers		CVE-2015-5237	8.8	2017-09-25	Unresolved	https://nvd.nist.gov/vuln/detail/
Protocol Buffers		CVE-2021-3121	8.6	2021-01-11	Unresolved	https://nvd.nist.gov/vuln/detail/
SnakeYAML	1.27	CVE-2022-1471	9.8	2022-12-01	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	5.3.1	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	5.3.1	CVE-2022-22965	9.8	2022-04-01	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	4.3.30	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	4.3.30	CVE-2022-22965	9.8	2022-04-01	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	4.3.19	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	4.3.19	CVE-2022-22965	9.8	2022-04-01	Unresolved	https://nvd.nist.gov/vuln/detail/
hazelcast	5.1	CVE-2022-0265	9.8	2022-03-03	Unresolved	https://nvd.nist.gov/vuln/detail/

Security탭 – Vulnerability Resolution

□ Vulnerability Resolution에 따른 Tab

- Fixed : Total 목록 중, Vulnerability Resolution이 'Fixed'로 변경된 CVE ID 목록만 확인 가능
- Not Fixed : Total 목록 중, Vulnerability Resolution이 'Fixed'가 아닌 CVE ID 목록 확인 가능

Total
Fixed
Not Fixed

Show Comment History Comment Edit ▾

Export Save

OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerability Link
~ <input type="text"/>	~ <input type="text"/>	~ <input type="text"/>	~ <input type="text"/>	~ <input type="text"/>	~ <input type="text"/>	~ <input type="text"/>
Protocol Buffers		CVE-2015-5237	8.8	2017-09-25	Unresolved	https://nvd.nist.gov/vuln/detail/
Protocol Buffers		CVE-2021-3121	8.6	2021-01-11	Unresolved	https://nvd.nist.gov/vuln/detail/
SnakeYAML	1.27	CVE-2022-1471	9.8	2022-12-01	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	5.3.1	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	5.3.1	CVE-2022-22965	9.8	2022-04-01	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	4.3.30	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	4.3.30	CVE-2022-22965	9.8	2022-04-01	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	4.3.19	CVE-2016-1000027	9.8	2020-01-02	Unresolved	https://nvd.nist.gov/vuln/detail/
Spring Framework	4.3.19	CVE-2022-22965	9.8	2022-04-01	Unresolved	https://nvd.nist.gov/vuln/detail/
hazelcast	5.1	CVE-2022-0265	9.8	2022-03-03	Unresolved	https://nvd.nist.gov/vuln/detail/

오픈소스
관리

보안취약점
관리

