

보안취약점 관리를 위한 Advanced Tip

24.11.12 석지영



보안취약점 데이터베이스

보안취약점 데이터베이스 수집

- 일 1회 NVD (NATIONAL VULNERABILITY DATABASE) 에서 제공되는 NVD Rest API (<https://nvd.nist.gov/developers/vulnerabilities>)를 통해 json 데이터 취득하여, Database에 저장
 - 최초 1회 API로 전체 NVD Data 취득하여 저장하며, 이후 최근 한 달전 단위로 변경된 데이터 취득하여 업데이트
- Vulnerability Score는 기본적으로 CVSS v3 Base Score를 기준으로 표기하며, CVSS v3 Score가 없는 경우 CVSS v2 Base Score를 대신해서 표기

보안취약점 데이터베이스와 OSS 매칭

- NVD CPE 데이터에서 product, version 값을 각각 OSS name(또는 nickname), OSS version 과 매칭하여 보안취약점 검출
 - CPE (common Platform Enumeration)란 운영 체제 및 소프트웨어 애플리케이션 식별하는 방법으로 다음과 같이 구성됨
 - cpe:2.3: part : vendor : product : version : update : edition : language : sw_edition : target_sw : target_hw : other

CVE-2022-22978 Detail

Current Description

In spring security versions prior to 5.4.11+, 5.5.7+ , 5.6.4+ and older unsupported versions, RegexRequestMatcher can easily be misconfigured to be bypassed on some servlet containers. Applications using RegexRequestMatcher with `.` in the regular expression are possibly vulnerable to an authorization bypass.

[+View Analysis Description](#)

Metrics CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

 **NIST: NVD** **Base Score:** 9.8 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Known Affected Software Configurations [Switch to CPE 2.2](#)

Configuration 1 ([hide](#))

Configuration	Up to (excluding)
cpe:2.3:a:vmware:spring_security:*:*:*:*:*:* Hide Matching CPE(s) <ul style="list-style-type: none"> cpe:2.3:a:vmware:spring_security:*:*:*:*:** cpe:2.3:a:vmware:spring_security:1.0.0:*:*:*:** cpe:2.3:a:vmware:spring_security:1.0.1:*:*:*:** cpe:2.3:a:vmware:spring_security:1.0.2:*:*:*:** 	5.5.7

보안취약점 데이터베이스와 OSS 매칭

- 예시 ([CVE-2022-22978](#))

Configuration 1 ([hide](#))

<pre>cpe:2.3:a:vmware:spring_security:*:*:*:*:*:*</pre> <p>Show Matching CPE(s) ▾</p>	Up to (excluding)	
	5.5.7	
<pre>cpe:2.3:a:vmware:spring_security:*:*:*:*:*:*</pre> <p>Hide Matching CPE(s) ▲</p> <ul style="list-style-type: none"> cpe:2.3:a:vmware:spring_security:5.6.0:*:*:*:*:* cpe:2.3:a:vmware:spring_security:5.6.1:*:*:*:*:* cpe:2.3:a:vmware:spring_security:5.6.2:*:*:*:*:* cpe:2.3:a:vmware:spring_security:5.6.3:*:*:*:*:* 	From (including)	Up to (excluding)
	5.6.0	5.6.4

Configuration 2 ([hide](#))

<pre>cpe:2.3:a:oracle:financial_services_crime_and_compliance_management_studio:8.0.8.2.0:*:*:*:*:*</pre> <p>Hide Matching CPE(s) ▲</p> <ul style="list-style-type: none"> cpe:2.3:a:oracle:financial_services_crime_and_compliance_management_studio:8.0.8.2.0:*:*:*:*:* 		
<pre>cpe:2.3:a:oracle:financial_services_crime_and_compliance_management_studio:8.0.8.3.0:*:*:*:*:*</pre> <p>Hide Matching CPE(s) ▲</p> <ul style="list-style-type: none"> cpe:2.3:a:oracle:financial_services_crime_and_compliance_management_studio:8.0.8.3.0:*:*:*:*:* 		

Configuration 3 ([hide](#))

<pre>cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:*:linux:*</pre> <p>Hide Matching CPE(s) ▲</p> <ul style="list-style-type: none"> cpe:2.3:a:netapp:active_iq_unified_manager:*:*:*:*:*:linux:* 		
--	--	--

<보안취약점 데이터베이스>

Product	version	CVSS
spring_security	5.6.0	9.8
spring_security	5.6.1	9.8
spring_security	5.6.2	9.8
spring_security	5.6.3	9.8
financial_services_crime_and_compliance_management_studio	8.0.8.2.0	9.8
financial_services_crime_and_compliance_management_studio	8.0.8.3.0	9.8
active_iq_unified_manager	-	9.8

보안취약점 데이터베이스와 OSS 매칭

- 예시 ([CVE-2022-22978](#))

Product	version	CVSS
spring_security	5.6.0	9.8
spring_security	5.6.1	9.8
spring_security	5.6.2	9.8

Open Source Information

OSS Name* i Rename **OSS Version**

Deactivate

Nickname

Add

org.springframework.security:spring-security-config ×	org.springframework.security:spring-security-core ×	org.springframework.security:spring-security-taglibs ×
org.springframework.security:spring-security-test ×	org.springframework.security:spring-security-web ×	Spring Security ×
Spring Security Config ×	Spring Security Core ×	Spring Security Taglibs ×
Spring Security Web ×	spring-projects-spring-security ×	spring-security-config ×
spring-security-core ×	spring-security-taglibs ×	spring-security-web ×

보안취약점 조회

Vulnerability List

- NVD 데이터 기준 수집된 보안취약점 검색 가능
 - FOSSLight Hub OSS DB에 등록되지 않았더라도 product명으로 검색 가능

	OSS Name	Nickname	OSS Version	Max CVSS Score	Vendor
	~ <input type="text"/> x	~ <input type="text"/> x	~ <input type="text"/> x	>= <input type="text"/> x	~ <input type="text"/> x
1	Apache Tomcat	tomcat	-	CRITICAL	apache
2	Apache Tomcat	tomcat	1.1.3	CRITICAL	apache
3	Apache Tomcat	tomcat	10.0.0	HIGH	apache
4	Apache Tomcat	tomcat	10.0.1	HIGH	apache
5	Apache Tomcat	tomcat	10.0.10	HIGH	apache
6	Apache Tomcat	tomcat	10.0.11	HIGH	apache

보안취약점이 검출된 OSS Name 또는 Product name으로 보안취약점 검출된 경우에 한하여,
또는 Product name (해당 product와 매칭된 OSS가 없는 경우) 을 표시

OSS List

- FOSSLight Hub에 저장된 OSS 검색을 통해 해당 OSS에 매칭된 취약점 확인 가능함

ID	OSS Name	OSS Version	License Name	Notice	Source	Vulnerability
11589	[Nick] xstream	1.4.9	BSD-3-Clause	✓		CRITICAL
3192	commons		Apache-2.0	✓		CRITICAL
45023	[Nick] spark	3.3.0	Apache-2.0	✓		CRITICAL
51907	[Nick] tiff	4.5.1	libtiff	✓		HIGH
32581	[Nick] Apache Tomcat	9.0.41	Apache-2.0	✓		HIGH

- OSS 상세 화면에서 해당 OSS (version)에 매칭된 전체 보안취약점 목록 확인 가능함

Vulnerability [+More](#)

CVE ID	NVD Score	Published Date
CVE-2023-44487	HIGH	2024-08-14 19:57:18
CVE-2023-46589	HIGH	2024-07-12 16:11:18
CVE-2021-42340	HIGH	2023-11-07 03:39:09
CVE-2021-41079	HIGH	2023-11-07 03:38:49
CVE-2021-25122	HIGH	2023-11-07 03:31:23

OSS 보안취약점 매칭 관리

OSS별 CPE 관리

Open Source Information 📄

OSS Name*

OSS Version

Nickname Add

Vulnerability Info ▼

Add

보안취약점 매칭을 위한 OSS version

Add

Add

보안취약점 매칭을 위한 추가 CPE

- vendor:product
- cpe:2.3:a:vendor:product:*:*:*:*:language:*:*

보안취약점 매칭 제외를 위한 CPE

보안취약점 매칭 version 예시

- CVE-2022-32207
 - product: curl, version: 7.81.0

Configuration 1 ([hide](#))

cpe:2.3:a:haxx:curl:*:*:*:*:*	From (including)	Up to (excluding)
Hide Matching CPE(s) ▲ <ul style="list-style-type: none"> • cpe:2.3:a:haxx:curl:7.69.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.69.1:*:*:*:* • cpe:2.3:a:haxx:curl:7.70.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.71.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.71.1:*:*:*:* • cpe:2.3:a:haxx:curl:7.72.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.73.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.74.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.75.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.76.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.76.1:*:*:*:* • cpe:2.3:a:haxx:curl:7.77.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.78.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.79.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.79.1:*:*:*:* • cpe:2.3:a:haxx:curl:7.80.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.81.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.82.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.83.0:*:*:*:* • cpe:2.3:a:haxx:curl:7.83.1:*:*:*:* 	7.69.0	7.84.0

보안취약점 매칭 version 예시

- Ubuntu 배포 버전 7.81.0-1ubuntu1.18 버전으로 OSS 관리하고 싶은 경우

Open Source Information

OSS Name i Rename

curl Deactivate

OSS Version 7.81.0-1ubuntu1.18

Nickname

Add

curl - curl x	curl-curl x	curl-libcurl x
curl_project-curl x	daniel_stenberg-curl x	haxx-curl x
libcurl x	libcurl-libcurl x	

Vulnerability Info v

OSS Version Alias Add

7.81.0 x

Include CPE Add	Exclude CPE Add
haxx:curl x	
daniel_stenberg:curl x	

Include CPE 예시

- CVE-2021-3121 (<https://github.com/gogo/protobuf/>)

<pre>cpe:2.3:a:golang:protobuf:*:*:*:*:*:*</pre> <p>Show Matching CPE(s) ▾</p>	<p>Up to (excluding)</p> <p>1.3.2</p>
--	---------------------------------------

- CVE-2021-22570 (<https://github.com/protocolbuffers/protobuf>)

Configuration 1 ([hide](#))

<pre>cpe:2.3:a:google:protobuf:*:*:*:*:*:*</pre> <p>Show Matching CPE(s) ▾</p>	<p>Up to (excluding)</p> <p>3.15.0</p>
--	--

- 이슈 case
 - Product명이 protobuf로 동일함
 - 기본적으로 두 CVE 모두 product 명과 일치하는 OSS name(또는 nickname)을 가지는 protobuf OSS와 매칭됨
 - protobuf Download Location : <https://github.com/protocolbuffers/protobuf>
 - 하지만 CVE-2021-3121는 golang-protobuf OSS와 매칭되어야 함
 - golang-protobuf Download Location : <https://github.com/gogo/protobuf/>

Include CPE 예시

- Golang-protobuf에 vendor:product (golang:protobuf) 입력함으로써 protobuf 대신 golang-protobuf와 CVE 매칭되도록 변경 가능

Open Source Information ↻ 📄 🗑️ 🔒

OSS Name* ℹ️ Rename **OSS Version**

golang-protobuf Deactivate 1.5.4

Nickname

Add

go:github.com/golang/protobuf × protobuf-protobuf ×

Vulnerability Info ▾

OSS Version Alias Add

Include CPE Add Exclude CPE Add

golang:protobuf ×

Include CPE 예시 (Full cpe)

- Vendor:product 값만으로 매칭 구별이 어려운 경우가 존재함
- CVE-2015-4411

Configuration 1 ([hide](#))

<pre>cpe:2.3:a:mongodb:bson:*:*:*:*:ruby:*:*</pre> <p>Show Matching CPE(s)▼</p>	Up to (excluding)
	3.0.4

- CVE-2020-7610

Configuration 1 ([hide](#))

<pre>cpe:2.3:a:mongodb:bson:*:*:*:*:node.js:*:*</pre> <p>Show Matching CPE(s)▼</p>	From (including)	Up to (excluding)
	1.0.0	1.1.4

Include CPE 예시 (Full cpe)

- bson-ruby OSS에 ruby language full cpe 추가

Open Source Information ↻ 📄 🗑️ 🔒

OSS Name* ℹ️ Rename **OSS Version**

Deactivate

Nickname

Add

×

Vulnerability Info ▾

Add

Add Add

×

×

Include CPE 예시

- js-bson OSS에 node.js language full cpe 추가

Open Source Information ↻ 📄 🗑️ 📁

OSS Name* ℹ️ Rename **OSS Version**

Deactivate

Nickname

Add

× × ×

Vulnerability Info ▾

Add

Add Add

×

Exclude CPE 예시

- CVE-2021-37701

Configuration 1 ([hide](#))

✖ cpe:2.3:a:npmjs:tar:*:*:*:*:node.js:*:* Show Matching CPE(s)▼	Up to (excluding) 4.4.16	
✖ cpe:2.3:a:npmjs:tar:*:*:*:*:node.js:*:* Show Matching CPE(s)▼	From (including) 5.0.0	Up to (excluding) 5.0.8
✖ cpe:2.3:a:npmjs:tar:*:*:*:*:node.js:*:* Show Matching CPE(s)▼	From (including) 6.0.0	Up to (excluding) 6.1.7

- 이슈 case

- 기본적으로 product명이 tar이므로 product 명과 일치하는 OSS name(또는 nickname)을 가지는 tar OSS와 매칭됨
- 하지만 npmjs:tar는 tar와 별개 OSS로 CVE 매칭에서 제외시키고 싶음

Exclude CPE 예시

- tar OSS에 vendor:product (npmjs:tar) 추가

Open Source Information ↻ 📄 🗑️ 🔒

OSS Name* ℹ️ v-Diff Rename **OSS Version**

tar Deactivate 1.34

Nickname

Add

Vulnerability Info ▾

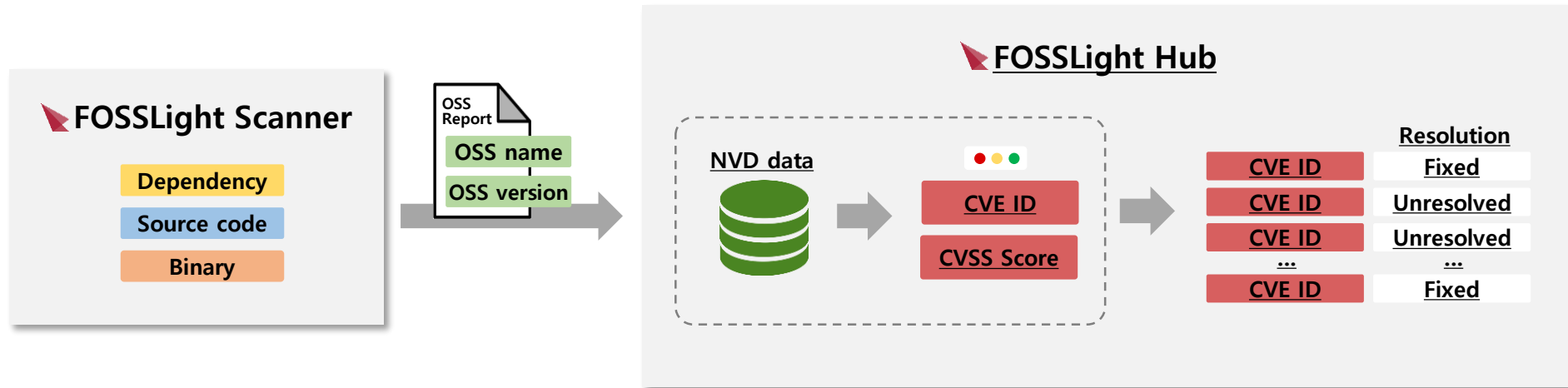
OSS Version Alias Add

Include CPE Add Exclude CPE Add

gnu:tar × npmjs:tar ×

프로젝트 별 보안취약점 관리

제품 보안취약점 수정 여부 관리 기능



Security탭 조치 여부 Score 관리

- System > Code management > 760 (Security Vulnerability Score)에서 변경 가능

FOSSLight

admin

Code management

Code No vulnerability

Code No	Code Name	Code Description
750	Vulnerability Mailing Score	Vulnerability Mailing Score Code
760	Security Vulnerability Score	Security Vulnerability Score Code

Page 1 of 1 15

Count: 2

Save

Detail No	Detail Name	Detail Description	Sub Code	Order	Use YN
100	Security Vulnerability Standard Score	5.0		1	Y

Count: 1

Code management

User management

History List

Notification

Sent Mail List

Help & Guide

Security탭

• Project List > Security탭


ID ▾	Project Name	Status	OSC Process	Download ⓘ	Security
747	datafile_collector	Progress	Identification > Packaging		Need to resolve(9.8)
737	test_sec_mail	Request	Identification > Packaging		Discovered(N/A)
736	Test empty project (1.0)	Request	Identification > Packaging		Discovered(N/A)
735	dep-test (1)	Request	Identification > Packaging		Discovered(N/A)
734	qwer (1.0)	Request	Identification > Packaging		Discovered(N/A)
733	test_prj	Request	Identification > Packaging		Need to resolve(9.9)
732	my_project_coffee	Request	Identification > Packaging		Need to resolve(9.8)
731	a123sdfs	Progress	Identification > Packaging		Need to resolve(7.5)

- **Need to resolve(10.0)** : Identification단계의 BOM 탭 기준 Security Vulnerability Score 이상 보안취약점이 존재하는 경우
- **Discovered(6.5)** : Identification단계의 BOM 탭 기준 Security Vulnerability Score 이상 보안취약점이 존재하지 않는 경우
- **Discovered(N/A)** : BOM탭이 merge and save되지 않아서 OSS 목록이 취합되지 않았거나 또는 보안취약점이 발견되지 않은 경우
- **Resolved (N/A)** : Need to resolve탭 기준 Security Vulnerability Score 이상 취약점이 모두 'Fixed' resolution인 경우
- 각 상태 (괄호) 안에서 프로젝트 내 vulnerability max score 확인 가능함




Security탭 > 취약점 취합 기준

- Project > Identification > BOM탭 save된 OSS 기준으로 Security탭에 보안취약점 취합

datafile collector | Progress | Identification > Packaging | Need to resolve(9.8)

3rd party DEP SRC BIN **BOM** 

OSS bulk registration Save (Binary DB)

+   

ID	Referenc	OSS Name	OSS Version	License	Download Locatio	Homepage	Copyright Text	Vulnera bility	Notice	Source	Restrictio	admin check <input type="checkbox"/>
		~ <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			
20	DEP	org.springdoc:springdoc-openapi-ui <small>Unconfirmed open source</small>	1.6.11	Apache-2.0	https://mvnrepository.com/artifact/org.springdoc/springdoc-openapi-ui/1.6.11	https://mvn			✓			<input type="checkbox"/>
18	DEP	org.springdoc:springdoc-openapi-ui <small>Unconfirmed open source</small>	1.6.11	Apache-2.0	https://mvnrepository.com/artifact/org.springdoc/springdoc-openapi-ui/1.6.11	https://mvn			✓			<input type="checkbox"/>
16	DEP	io.netty.incubator/netty-incubator-transport-native-epoll <small>Unconfirmed open source</small>	0.0.28	Apache-2.0	https://mvnrepository.com/artifact/io.netty.incubator/netty-incubator-transport-native-epoll/0.0.28	https://mvn			✓			<input type="checkbox"/>
17	DEP	io.netty.incubator/netty-incubator-transport-native-epoll <small>Unconfirmed open source</small>	0.0.28	Apache-2.0	https://mvnrepository.com/artifact/io.netty.incubator/netty-incubator-transport-native-epoll/0.0.28	https://mvn			✓			<input type="checkbox"/>

Need to resolve / Full discovered 탭 (신규 Update)

- Need to resolve : Security Vulnerability Score 이상인 CVE ID 목록 확인 가능
- Full Discovered : Identification 단계의 BOM 탭 기준 OSS 대상으로 검출된 전체 CVE ID 목록

Need to resolve
Full Discovered
🔒

A list of CVE IDs with a vulnerability score of 5.0 or higher for OSS targets based on the BOM tab in the Identification step.

FOSSLight Security Report

Upload Drag & Drop Files

+ 🗑️ ✎ 📄

☐	OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerability Link	Security Comments
	~ 🔍	x ~ 🔍	x ~ 🔍	x ~ 🔍	x ~ 🔍	x ~ 🔍	x ~ 🔍	x ~ 🔍
☐	Apache Commons Text	1.9	CVE-2022-42889	9.8	2022-10-13	Unresolved	https://nvd.nist.gov/vuln/detail	
☐	jackson-dataformats-text	2.13.3	CVE-2023-3894	7.5	2023-08-08	Unresolved	https://nvd.nist.gov/vuln/detail	
☐	mockserver	5.11.2	CVE-2021-32827	9.6	2021-08-16	Unresolved	https://nvd.nist.gov/vuln/detail	
☐	Netty	4.1.79	CVE-2022-41881	7.5	2022-12-12	Unresolved	https://nvd.nist.gov/vuln/detail	

Excel 업로드 기능 (신규 Update)

- 업로드된 Excel파일 내 OSS name, OSS version, CVE ID값이 동일한 경우, upload한 데이터 중 Vulnerability resolution, Security Comments 값을 load

Need to resolve Full Discovered

A list of CVE IDs with a vulnerability score of 5.0 or higher for OSS targets based on the BOM tab in the Identification step.

FOSSLight Security Report

Upload Drag & Drop Files

해당 컬럼만
엑셀 값으로
로드 가능

<input type="checkbox"/>	OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution	Vulnerability Link	Security Comments
~	<input type="text"/>	x	<input type="text"/>	x	<input type="text"/>	x	<input type="text"/>	x
<input type="checkbox"/>	Apache Commons Text	1.9	CVE-2022-42889	9.8	2022-10-13	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2022-42889	
<input type="checkbox"/>	jackson-dataformats-text	2.13.3	CVE-2023-3894	7.5	2023-08-08	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2023-3894	
<input type="checkbox"/>	mockserver	5.11.2	CVE-2021-32827	9.6	2021-08-16	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2021-32827	
<input type="checkbox"/>	Netty	4.1.79	CVE-2022-41881	7.5	2022-12-12	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2022-41881	
<input type="checkbox"/>	slf4J	1.7.25	CVE-2018-8088	9.8	2018-03-20	Unresolved	https://nvd.nist.gov/vuln/detail/CVE-2018-8088	

Security탭 조치 여부와 Identification 연동

- Security탭에서 Fixed 처리된 CVE ID에 대해 Identification탭에서 제외하고 vulnerability max score 확인 가능

OSS Name	OSS Version	CVE ID	CVSS SCORE	Published Date	Vulnerability Resolution
~ <input type="text"/>	x	~ <input type="text"/>	x	~ <input type="text"/>	x
SnakeYAML	1.30	CVE-2022-1471	9.8	2022-12-01	Fixed
SnakeYAML	1.30	CVE-2022-25857	7.5	2022-08-30	Fixed
SnakeYAML	1.30	CVE-2022-38751	6.5	2022-09-05	Fixed
SnakeYAML	1.30	CVE-2022-38749	6.5	2022-09-05	Fixed
SnakeYAML	1.30	CVE-2022-41854	6.5	2022-11-11	Fixed
SnakeYAML	1.30	CVE-2022-38752	6.5	2022-09-05	Fixed
SnakeYAML	1.30	CVE-2022-38750	5.5	2022-09-05	Unresolved

Security탭 조치 여부와 Identification 연동

- Security탭에서 Fixed 처리된 CVE ID에 대해 Identification탭에서 제외하고 vulnerability max score 확인 가능

The screenshot displays the FOSSlight interface with two main panels. The left panel shows the 'BOM' tab with a table of components. The right panel shows the 'Identification' tab with a table of vulnerabilities.

Left Panel (BOM Table):

ID	Referenc	OSS Name	OSS Version	License
106	DEP	SnakeYAML	1.30 <i>Unconfirmed vers</i>	Apache-2.0

Right Panel (Vulnerability Table):

	OSS Name	Version	Score	CVE ID	Modified Date
1	snakeyaml	1.30	5.5	CVE-2022-38750	2024-03-15
2	snakeyaml	1.30	9.8	CVE-2022-1471	2024-06-21
3	snakeyaml	1.30	7.5	CVE-2022-25857	2024-03-15
4	snakeyaml	1.30	6.5	CVE-2022-38749	2024-03-15
5	snakeyaml	1.30	6.5	CVE-2022-38751	2024-03-15
6	snakeyaml	1.30	6.5	CVE-2022-38752	2024-03-15
7	snakeyaml	1.30	6.5	CVE-2022-41854	2024-06-21

The table in the right panel has a red border around rows 2 through 7, indicating they are filtered out of the Security tab. The bottom of the interface shows pagination: Page 1 of 0, 200 items per page, and Total: 7.

보안취약점 메일링

메일링 기준 Score 관리

- System > Code management > 750 (Vulnerability Mailing Score)에서 변경 가능

FOSSLight

admin

Dashboard

License

Open Source

Project

3rd Party

Binary DB

Vulnerability

Self-Check

User Settings

System

Statistics

Code management

User management

History List

Notification

Sent Mail List

Help & Guide

Vulnerability Log

BinaryDB Log

Code No vulnerability

Code No	Code Name	Code Description
750	Vulnerability Mailing Score	Vulnerability Mailing Score Code
760	Security Vulnerability Score	Security Vulnerability Score Code

Page 1 of 1 15

Count: 2

Save

Detail No	Detail Name	Detail Description	Sub Code	Order	Use YN
100	Vulnerability Mailing Standard Score	5.0		1	Y

Count: 1

Delete

보안취약점 실시간 알림

- Vulnerability Mailing Score 이상 CVSS Score를 가지는 신규 CVE ID 발견 시, 해당 CVE ID와 매칭된 OSS가 사용된 프로젝트 담당자에게 'Discovered' 메일 알림

FOSSLight Hub Notification

[OSC] Vulnerability Discovered

« Vulnerability Information »

OSS ID	OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
22869	json-smart-v2	2.2.1	CVE-2021-27568	9.1	An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as demonstrated by NumberFormatException. When it is not caught, it may cause programs using the library to crash or expose sensitive information.	2021-02-23	2022-05-12
15690	json-smart-v2	2.3	CVE-2021-27568	9.1	An issue was discovered in netplex json-smart-v1 through 2015-10-23 and json-smart-v2 through 2.4. An exception is thrown from a function, but it is not caught, as demonstrated by NumberFormatException. When it is not caught, it may cause programs using the library to crash or expose sensitive information.	2021-02-23	2022-05-12

* This mail was sent by osc.lge.com

보안취약점 실시간 알림

- Vulnerability Mailing Score 이하로 CVE ID의 CVSS Score 변경 시, 해당 CVE ID와 매칭된 OSS가 사용된 프로젝트 담당자에게 'Recalculated' 메일 알림

FOSSLight Hub Notification

[OSC] Vulnerability Recalculated

« Vulnerability Information »

OSS ID	OSS Name	OSS Version	CVE ID	Score	Summary	Published Date	Modified Date
83203	director		CVE-2010-0128 -> NONE	9.3 -> 0.0			
24445	python-babel-babel	2.8.0	CVE-2021-42771 -> NONE	7.8 -> 0.0			

* This mail was sent by <http://osc.lge.com>

메일링 Enable/Disable 설정

- Project Information > Security Mail (Vulnerability)에서 설정 가능

Project Information 🔗 📄 🗑️ 📁

Project Name* **Project Version** **Priority*** ✕ ▼

Permission

Security Mail (Vulnerability)

Operating System* ✕ ▼ **Distribution Type*** ✕ ▼

Network service only? Yes No

Model Information <



감사합니다

