

KYLIN-5357

Dev Design

Fix new high-risk vulnerability CVE-2022-31692

需要修复 Spring Security 高危漏洞CVE-2022-31692，受影响的组件版本如下：

- 5.6.0 <= Spring Security <= 5.6.8
- 5.7.0 <= Spring Security <= 5.7.4

已核实该漏洞的等级为高危（CVSS 3.x 评分 7.4）

How to fix

将 kylin root pom 中的 `spring-security-web` 版本 `5.6.4` → `5.6.9`

Fix new high-risk vulnerability CVE-2022-23221

Upgrade `com.h2database:h2` to version 2.1.210 or higher.

How to fix

1. 升级 `com.h2database` `1.4.197` -> `2.1.214`
2. kylin-server、ke-smart-booter 模块依赖的 `com.h2database` scope 改为 test

Fix new high-risk vulnerability CVE-2022-23457

Upgrade `org.owasp.esapi:esapi` to version 2.3.0.0 or higher.

How to fix

按照官方的做法，2.3.0.0 版本已经修复漏洞

所以在 kylin root pom 中新增以下依赖即可覆盖 `spring-security-saml2-core:1.0.10.RELEASE` 中的 `org.owasp.esapi:esapi:2.2.0.0`

```
1 <esapi.version>2.3.0.0</esapi.version>
2
3 <dependency>
4     <groupId>org.owasp.esapi</groupId>
5     <artifactId>esapi</artifactId>
6     <version>${esapi.version}</version>
7 </dependency>
```

Fix new high-risk vulnerability CVE-2022-34169

how to fix

1. 将 `spring-security-saml2-core` 依赖的 `xalan` 给 exclude 掉。
2. `kylin-it` 模块下的依赖了 `xalan` `scope test`，删掉依赖。