Log4j2 漏洞复现及解决方案

原创

HiiZack 于 2021-12-15 16:09:27 发布 2369 收藏
分类专栏： Java 文章标签： 安全 web安全 log4j2 日志框架

背景

> 最近IT圈爆出的 Apache Log4j2 存在重大安全漏洞问题，当 Log4j2 版本在 2.15.0 以前（2.0 <= V <= 2.14.1），相关应用程序或中间件如 ES、Redis 等均会受此漏洞影响。不过目前 apache 官方已经修复了此漏洞。

漏洞复现程序

Log4j2 lookup 漏洞复现程序

修复指南

推荐修复指南1：升级 log4j2 接口及实现版本至最新版（2.15.0）

```
<dependencies>
    <!-- log4j2 facade, fixed 2.15.0 -->
    <dependency>
        <groupId>org.apache.logging.log4j</groupId>
        <artifactId>log4j-api</artifactId>
        <version>2.15.0</version>
    </dependency>

    <!-- log4j2 core, fixed 2.15.0 -->
    <dependency>
       <groupId>org.apache.logging.log4j</groupId>
        <artifactId>log4j-core</artifactId>
        <version>2.15.0</version>
    </dependency>
</dependencies>
```

此方式适用于项目中有直接依赖 log4j2 的工程，直接升级到最新版本，保留 log4j2 的特性与性能要求。

推荐修复指南2：使用桥接器将log4j桥接到slf2j

```
<!-- log4j桥接到slf4j -->
<dependency>
   <groupId>org.apache.logging.log4j</groupId>
   <artifactId>log4j-to-slf4j</artifactId>
   <version>2.15.0</version>
</dependency>

<!-- jul桥接到slf4j -->
<dependency>
   <groupId>org.slf4j</groupId>
   <artifactId>jul-to-slf4j</artifactId>
   <version>1.7.25</version>
   <scope>compile</scope>
</dependency>
```

此方式的好处在于，实际项目中，可能存在各种各样的日志框架，为了方便管理，可以将其它日志框架统一桥接到 sl4j上，然后使用 logback 打印日志。此方式也适用于各种中间件对 log4j2的依赖。而不好的点在于，桥接到其它的日志框架之后，会牺牲 log4j2高性能特性。