**蓝源卫士**

Blue Guardian

**白皮书**

江西省蓝源科技股份有限公司

2022年

目 录

[一、 背景分析 1](#_Toc10093)

[ Log4j2漏洞事件 2](#_Toc12984)

[二、 许可证合规及兼容风险 3](#_Toc943)

[ 软件许可证(license) 3](#_Toc824)

[ 许可证风险 3](#_Toc3201)

[三、 局势分析 5](#_Toc31589)

[ 开源组件的独立性 5](#_Toc26414)

[ 已知漏洞 5](#_Toc12388)

[ 安全隐患 5](#_Toc19775)

[ 漏洞影响范围广大 5](#_Toc29358)

[ 维护与代码衰退 6](#_Toc7694)

[ 软件成分分析工具不可或缺 6](#_Toc22992)

[四、 蓝源卫士的功能与特色 7](#_Toc31255)

[ 主要功能 7](#_Toc14095)

[ 丰富的资源储备 7](#_Toc7534)

[ 高效的匹配技术 7](#_Toc28270)

[ 多样化报表呈现 7](#_Toc6981)

[ 多层次安全检测 8](#_Toc28841)

[ 易用性 8](#_Toc27254)

[ UI界面 8](#_Toc9747)

[ 漏洞修复 8](#_Toc29534)

1. 背景分析

几年前，开源还是点点星火，如今已成燎原之势。自2018年起，企业都在积极加强自己在开源方面的实力，如:IBM大手笔340亿美元收购了RedHat,微软75亿美元收购了GitHub。从这点我们可以看出开源组件对于现代软件开发的重要性和日益显著的使用需求。而事实便是如此，据 GitHub 报告称，仅2018 年一年新用户的注册量就已经超过了之前六年的总和，且平台上创建的新组织和新存储库增加了 40%。另外，开源软件同时也推动了语言和平台的发展，影响了行业增长，Forrester 报告称，开源软件是业务技术战略的重要组成部分。

科技公司都在大量使用开源，每个编程语言生态系统中都有越来越多的开源库被索引，以2017年到2018年来说，有的增长率已经达到了两位数甚至是三位数的增长(Maven Central实现了102%的三位数增长),仅2018年java包增加了一倍，NPM增加了大约250000个新包。

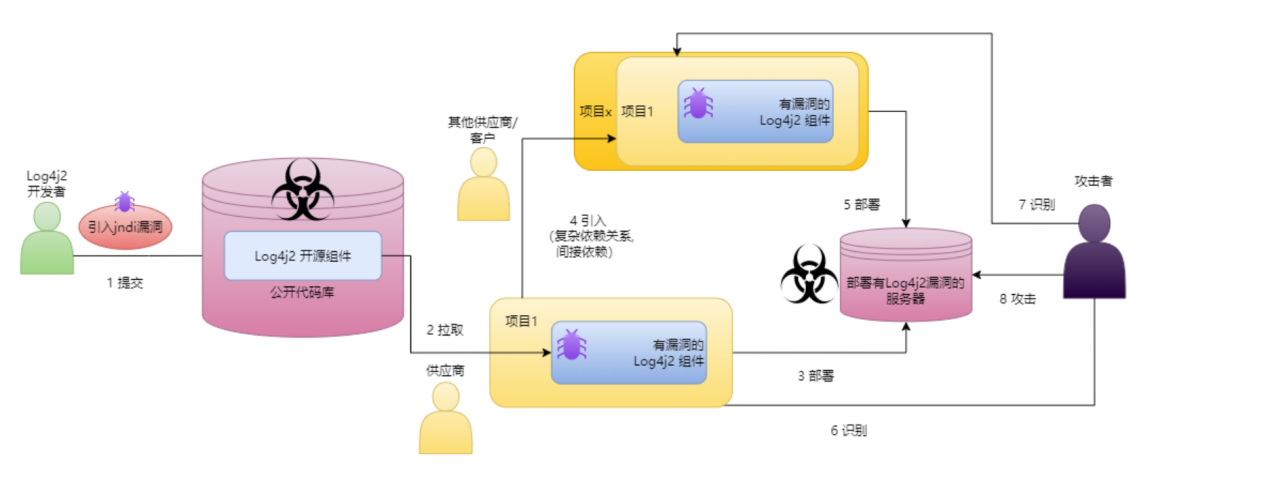
但是，仅在 2018 年内，在开源社区内就已经暴露出 16,555 个新的漏洞，而总漏洞数也突破了 10 万的关口。此外，在 2018 年内，谷歌、Facebook 和亚马逊等科技巨头也相继披露了至少 1 起网络安全意外事故。如果我们再将时间轴往后推进，在近 5 年内， 也发生了一些通过利用开源漏洞导致在应用程序中造成灾难性威胁的安全漏洞如：Heartbleed （5 亿美元），Panama Papers 和 Equifax（4.39 亿美元）等事件。所以毫无疑问的，开源软件的安全性将成为开发人员极具关注的一项课题。随着开源的日益普及，开源软件的安全性也将成为更严苛，更复杂的挑战，开源组件的使用率预计将从2018年的1200万增长到2026年的3亿。

虽然开源有其优势，但其风险也是显著的， 开源项目的可更改性和便利性，都可能成为黑客的首选攻击点。因此，开发人员有必要确保他们所使用的开源组件的安全性，并持续监控这些组件的安全漏洞问题。此外， 许多的开源组件都附带着许多隐藏条款，或是许可证等，这些都有可能导致企业深陷 法律诉讼的泥沼。

综上所述，不论是开发人员对于开源组件的监控需求，企业对于开源组件的安全性和法律风险的担忧，对于开源软件的分析和监控是必要的，而蓝源卫士也是应需而生。

* **Log4j2漏洞事件**

Apache Log4j2 是一个开源基础日志库，作为 Log4j 组件的升级版本广泛应用于软件项目的开发、测试和生产，在 Maven Repository 中被接近 7000 个项目引用。Log4j2 具有“PropertySupport”特性，该特性在打印日志时支持从配置文件、系统变量、环境变量、线程 Context以及事件中存在的数据中引用所需的变量到日志中。而在支持该特性的 org.apache.logging.log4j.core.lookup 包中提供了一系列的插件，允许用户从自定义渠道获取属性。而问题就在于包中的 JndiLookup 插件允许用户通过 JNDI 进行变量的检索，但是未对查询地址做好过滤，导致产生 JNDI 注入漏洞，从而造成代码执行、命令执行等风险。对于开源组件，自身漏洞对整个软件供应链的影响最为直接、隐秘且长久。Log4j2 作为一个堪比标准库的基础日志库，受众极其广泛，也就导致漏洞的影响范围极大，再加上此次曝出的漏洞利用难度低（默认配置即可利用），在曝光开始就吸引了整个行业的注意。



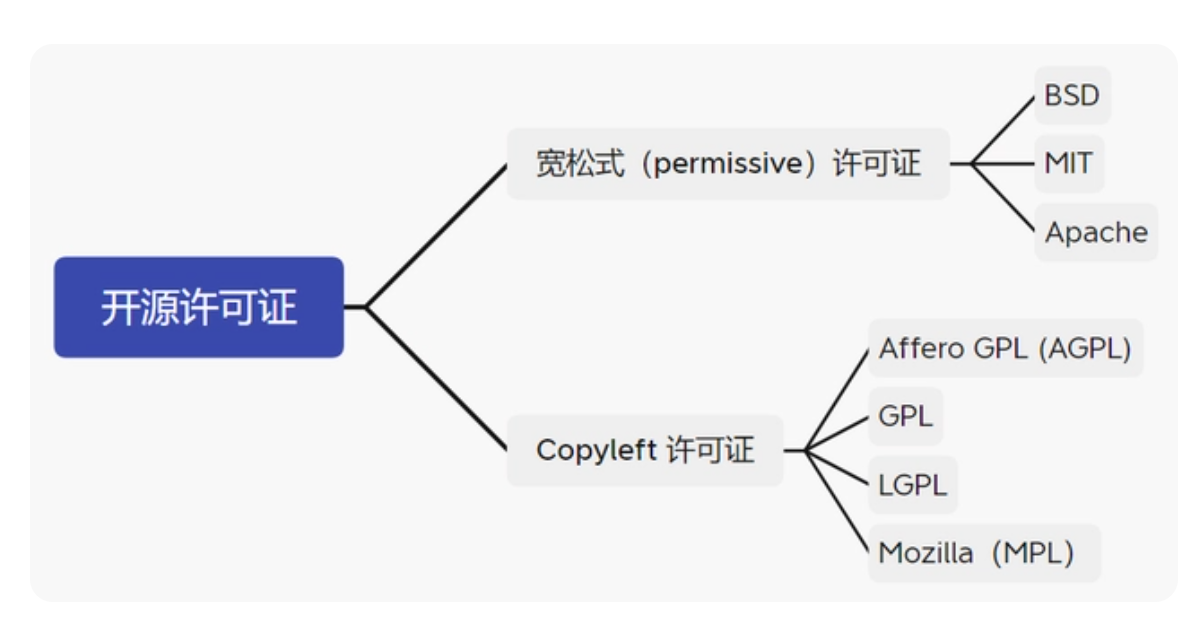
**图1** Log4j2事件潜在攻击流程图

Log4j2 漏洞之所以影响严重，是因为它在许多项目中以基础设施的身份存在。随着项目结构体积逐渐庞大，引入组件的来源增多，项目结构、依赖关系也越加复杂，也就越难发现隐藏较深的间接组件。相比针对开源机制的攻击手段，比如开发工具污染、依赖混淆等，依靠企业现有技术手段很难规避这类间接组件漏洞风险，重点应放在应急响应上。在漏洞曝出的第一时间，基于开源软件成分清单识别间接组件漏洞，对于快速研判影响、制定决策至关重要。

1. 许可证合规及兼容风险

* **软件许可证(license)**

目前业界中有超过400种不同类型的开源许可证，仍然有大部分的人误以为”开源=免费”。开源软件对用户是免费的，但并不意味着可以在不遵守其它义务的情况下使用。随着开源技术的发展，结合各自需要，开源软件一般都有对应的开源许可证（Open Source License），用以对软件的使用、复制、修改和再发布等进行限制。常见的开源软件许可证根据开放程度可以大致分为两大类：宽松自由软件许可协议（“Permissive Free Software Licence”）和著作权许可证（“Copyleft License”）。宽松自由软件许可协议包括 MIT、Apache、BSD 等，允许用户自由复制、修改、许可和再许可代码，开源软件源代码变更或衍生软件可以变为专有软件；著作权许可证包括 GPL 许可证、MPL 许可证和 LGPL 许可证等，强制要求公开源代码变更或衍生软件开源。



**图2** 软件开源许可证

* **许可证风险**

Contrast Security 发布的《2021 State of Open-Source Security Report》报告中相关数据表明，几乎所有（99%）的组织都至少有一个高风险的 Java 许可证，69% 的 Java 应用程序和 33% 的 Node 应用程序中至少存在一个高风险许可证，95% 的 Java 应用程序和 70% 的 Node 应用程序至少存在一个未知或可变风险的许可证。如果不了解开源软件的知识产权或未按照开源许可证使用开源软件，很可能侵犯他人知识产权，引起法律纠纷，面临重大风险。同时开源软件可能存在层层依赖关系，企业组织在使用开源过程中不断加入新的开源组件，可能存在许可证不兼容的风险。

2021年12月，抖音海外版 TikTok 上线了一款名为 TikTok Live Studio 的 APP，但不久其下载页面就被删除。TikTok 官方对此事做出回应，原因是该 APP 违反 GPL 许可证，其使用 GPL 许可证下的开源软件源码，却没有按照 GPL 许可证要求开源。

随着开源软件的发展，其数量和影响力在不断地上升。开源软件具有成本低、升级快的特点，因此越来越多的企业选择使用开源软件。但是“天下没有免费的午餐”，在开源许可证的约束下，开源软件的使用并非想象中的自由。不恰当地使用开源软件，可能会给企业造成负面舆论甚至经济损失的风险。所以对于许可证的合规性检测也是开发中不可或缺的过程。

1. 局势分析

* **开源组件的独立性**

现今的大部分应用程序，无论是移动应用程序，网页应用程序或是桌面应用程序 等，都已不再是从头一步一步的编写，而是开发者利用开源组件和第三方库协助开发。 虽然这极大的简化了开发过程，以及产品的面世时间，但与此同时，使用开源组件也 将让用户所处的机构曝露在各种不同的外在风险之中。

* **已知漏洞**

由 NVD 数据库 (National Vulnerabilities Database) 所维护超过 100,000 个 CVE 是最广为人知的漏洞数据库。任何人皆可通过简单的网络搜索来寻找发现这些漏洞并加以 利用，这些漏洞亦能成为黑客为之利用的系统突破口，Equifax 事件正好可以作为该情况的前车之鉴。

* **安全隐患**

NVD 数据库已然是一个进行攻击的很好的突破口，但实际情况中有更多数量的漏 洞被第三方开发人员私下发现并修复。这些未曾被公开的 “安全隐患” 若被加以利用， 其可能对系统造的损害并不小于其他漏洞所带来的损害。

* **漏洞影响范围广大**

开源软件因其开放、自由、共享等特性，开源技术可以从代码托管平台、技术社区、开源机构官方网站等渠道获取，或通过合作研发、商业采购等方式引入开源代码、开源组件、开源软件和基于开源技术的云服务等。开源社区参与者广泛分布于全球各地，没有中央权威来收录漏洞信息，保证开源软件的质量和维护。开发人员不了解开源软件信息，缺少漏洞跟踪能力，漏洞修复时间滞后，增加了软件供应链安全治理难度。本质上来讲，开源软件并不比自定义代码更安全，与任何软件一样，它可能包含导致安全问题的漏洞。而且，大部分软件开发人员在引入第三方库的时候，并没有关注引入组件是否存在安全隐患或者缺陷，并且由于开源软件之间的关联依赖关系错综复杂，一旦开源软件存有恶意代码或病毒，将会产生蝴蝶效应，导致所有与之存在关联依赖关系的其他软件系统出现同样的漏洞，漏洞的攻击面由点及面呈现出爆炸式的放大效果，给用户带来严重危害。

* **维护与代码衰退**

理论上，具有较高安全意识的开发人员能够确保他们所使用的库或组件在开发时并不存在任何漏洞或是安全隐患问题，但现实情况是，没有任何人能够保证系统在整个软件周期中的永久安全性。每一年都有将近 15,000 个新的漏洞被发现，这也就是为 何任何 “安全” 的软件，都终将面临 “代码衰退” 的问题，让其从不可能变成可能，增加其被攻击的概率。

* **软件成分分析工具不可或缺**

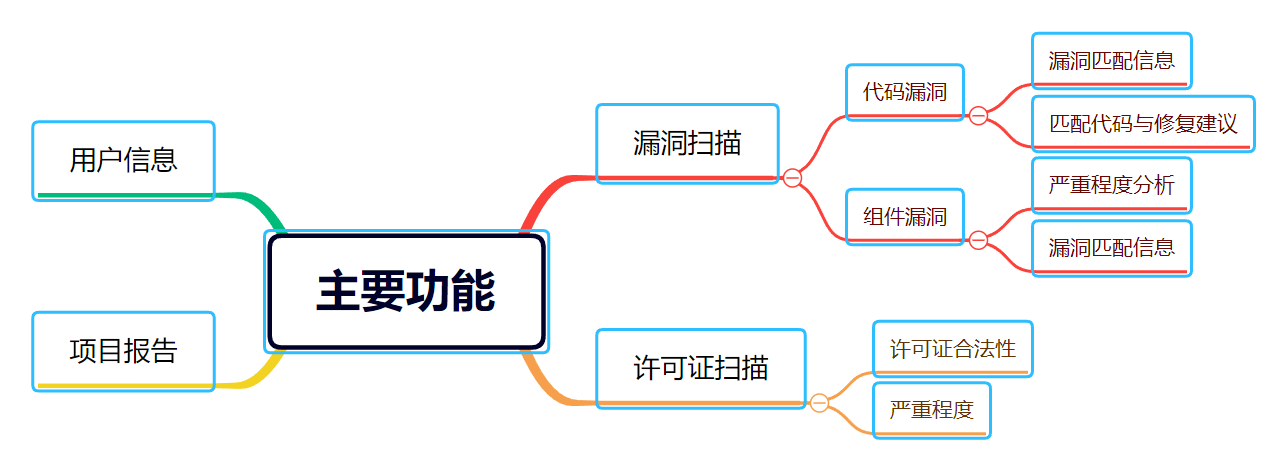
综上所述，在现今要求高效高产出的软件开发环境中，开发人员普遍上使用甚至依赖于开源组件或是第三方库的协助，以降低开发所需时间和成本。然而，在开发人员开发时对于这些开源组件和第三方库的使用，在无形中可能为软件或是企业本身埋下不可预测的安全炸弹或是带来其他许可证风险，在这样一个环境的推动下，业界对于软件成分分析工具的需求显著增长。

1. 蓝源卫士的功能与特色

蓝源卫士是一个注重于漏洞扫描分析，许可证扫描分析且支持源代码扫描的一款智能软件成分分析工具。蓝源卫士通过利用已知开源组件的特征，匹配和分析程序所使用的开源组件，并与已收录漏洞进行匹配对比，识别所存有的安全隐患问题并提供漏洞修补建议。

* **主要功能**

蓝源卫士依据CVE(Common Vulnerabilities & Exposures)公共漏洞字典表、OWASP Web漏洞，以及设备、软件厂商公布的漏洞库，结合专业源代码扫描工具对各种程序语言编写的源代码进行安全审计。能够为客户提供包括安全编码规范咨询、源代码安全现状测评、定位源代码中存在的安全漏洞、分析漏洞风险、给出修改建议、许可证证书合法性判断等一系列服务。



**图3** 蓝源卫士主要功能

* **丰富的资源储备**

拥有60+T开源代码匹配仓库，2800万+ 开源匹配项目，1.9亿+ 开源匹配组件，180000+开源匹配漏洞。

* **高效的匹配技术**

依赖片段代码哈希值进行特征向量匹配算法，单个文件哈希值进行特征向量匹配算法,通用项目文件依赖匹配算法，可进行快速准确检测安全漏洞问题。

* **多样化报表呈现**

以图，表，文字说明等多种形式进行结果报表展现，同时支持excel格式导出结果报表。

* **多层次安全检测**

能够检测系统安全，网页编程安全，sql注入，跨站漏洞等各个方面的安全漏洞。

* **易用性**

对于使用蓝源卫士的用户，我们的工具上手简单，只需要用户将程序压缩包导入工具中，无需做其他操作，蓝源卫士会自动扫描匹配漏洞与许可证信息，以不同形式展示，以便用户查看。

* **UI界面**

蓝源卫士界面简介明快，提示准确到位，必要的变动操作有二次确认操作，给用户带来良好的使用体验。

* **漏洞修复**

得益于特征向量匹配算法，蓝源卫士除了能够准确匹配漏洞信息以外，还能够提供相应的漏洞修复建议。另外还能够对于漏洞信息快速定位。