
GOTC 2023
全球开源技术峰会
THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE
OPEN SOURCE, INTO THE FUTURE
快闪演讲
本期议题：openBrain开源漏洞感知系统
杨牧天 2023年05月28日

About

openBrain（微知）开源漏洞感知系统是基于**“源图”开源软件供应链重大基础设施**打造的面向开源社区的安全漏洞情报跟踪与分析系统。

openBrain依据开源社区中软件物料清单，在全球范围监测相关漏洞情报，并实现多源多类情报汇总、处置优先级评估、漏洞影响主体软件识别、早期漏洞灰度检测、疑似漏洞预警、验证程序及修复方案推荐等能力，提升开源社区对开源软件供应链漏洞情报的获取能力和漏洞处置效率。

目录

技术概述

技术进展

应用扩展

目录

技术概述

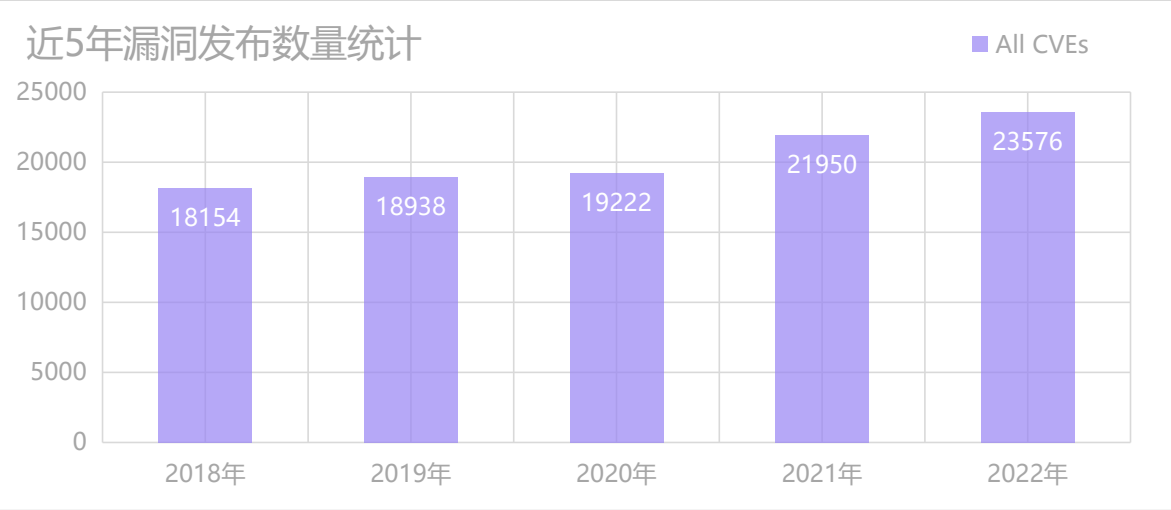
技术进展

应用扩展

现象和问题

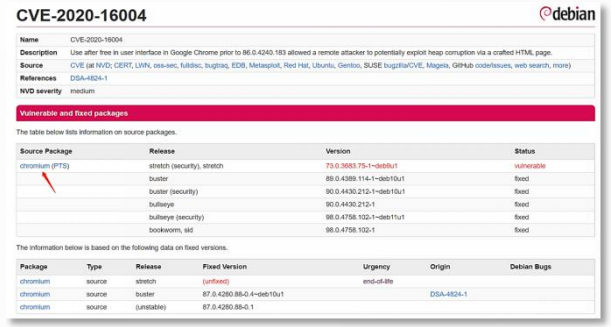
漏洞基数庞大

安全漏洞披露数量逐年增多，开源软件漏洞持续增多。



情报质量不足

漏洞情报同时也存在缺、错、慢的问题，开源社区需要更高效、低成本的漏洞情报获取能力。



供应链关系复杂

众多开源项目包含复杂的开源软件供应链关系，从海量漏洞和海量开源组件中寻找与项目相关的情报成本较高。

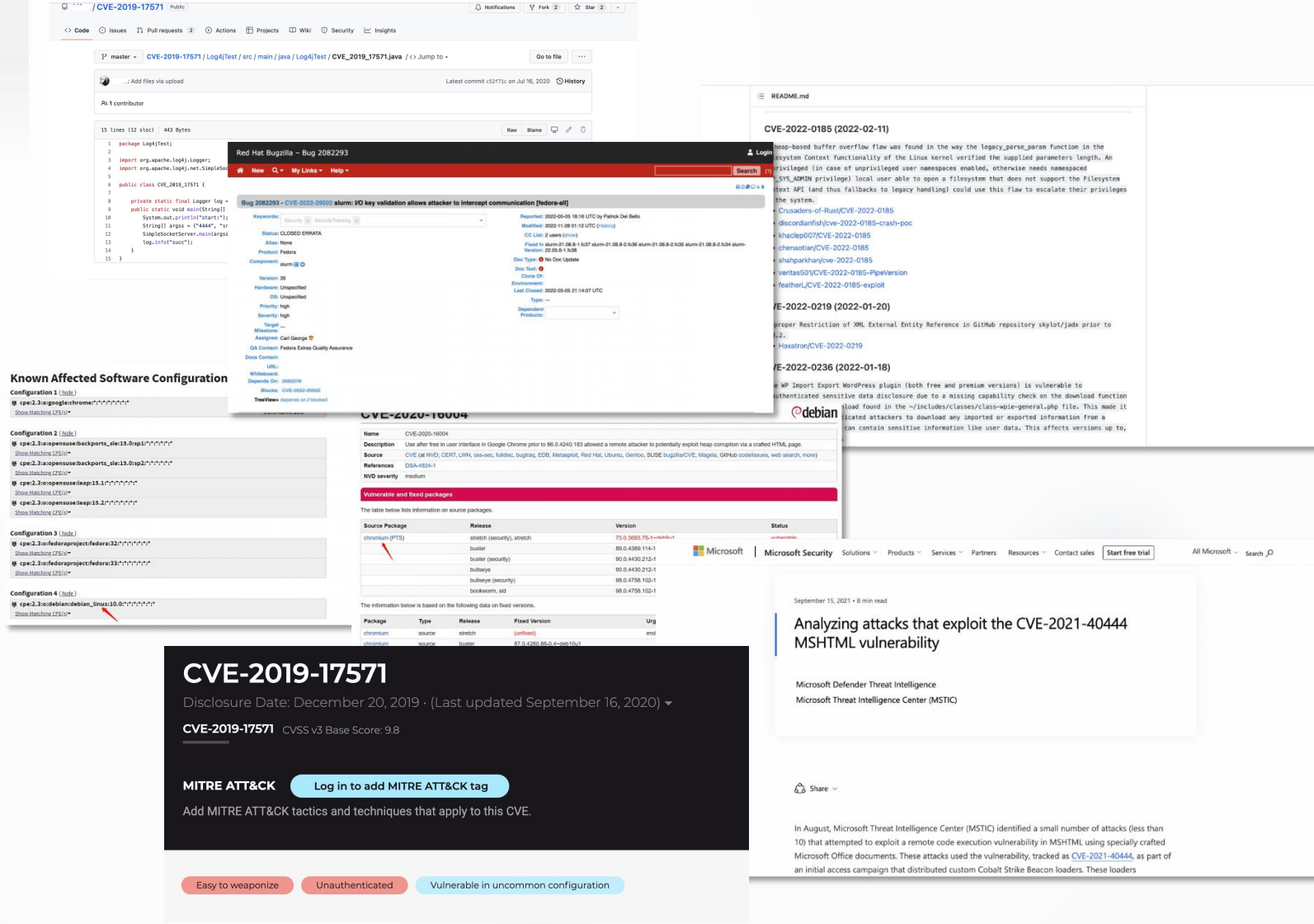
开源安全知识获取与处理

现象和问题

漏洞情报分散

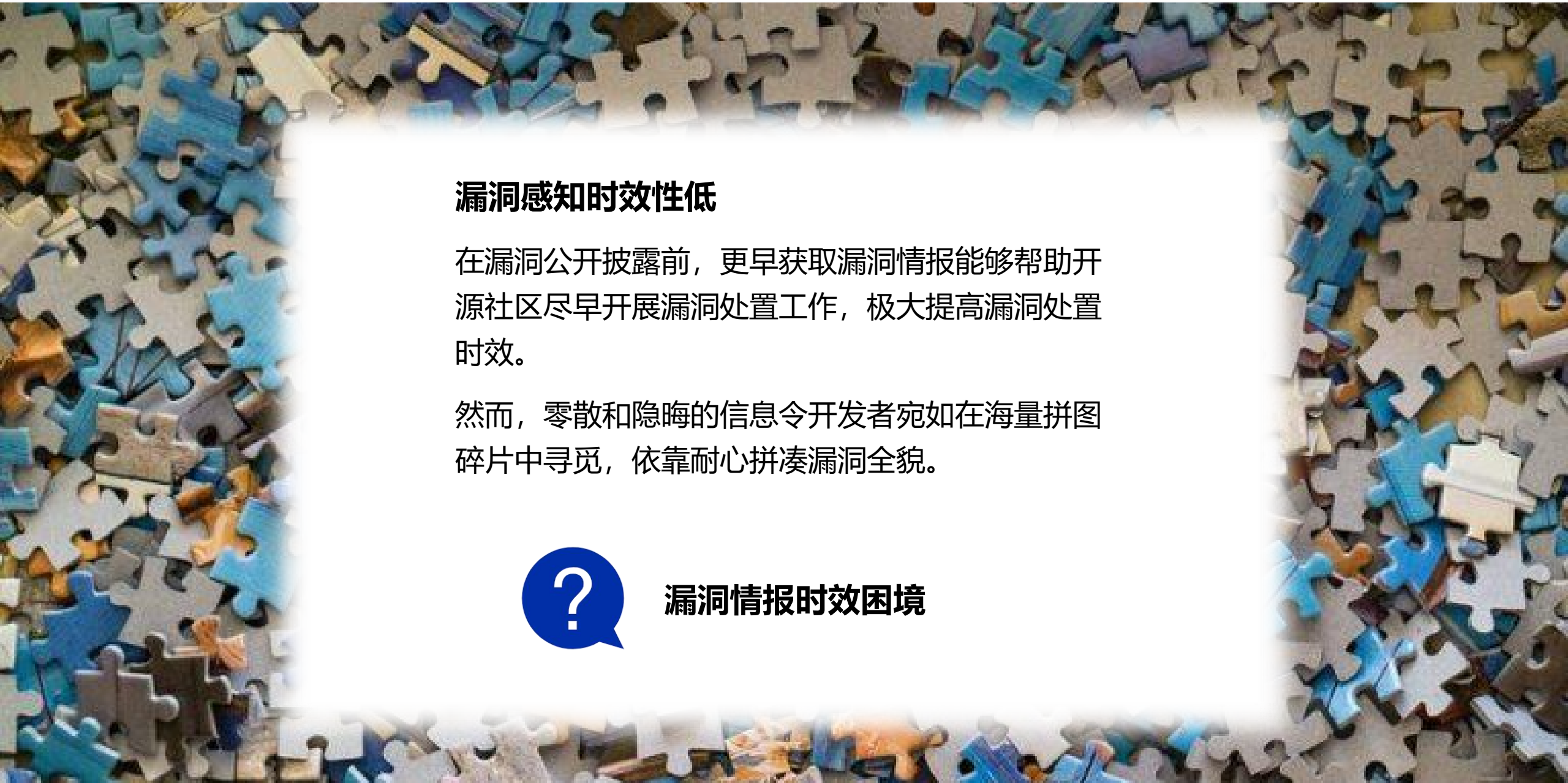
不同维度的漏洞情报分散在大量不同数据源，需要人工阅读、分析、理解，寻找关键知识并提取知识间的联系，需要较高的经验和时间成本。

并非每个开源贡献者都是安全专家，开源社区需要漏洞情报的自动化知识提取、关联与分析技术，以降低人工参与环节。



分散情报融合

现象和问题



漏洞感知时效性低

在漏洞公开披露前，更早获取漏洞情报能够帮助开源社区尽早开展漏洞处置工作，极大提高漏洞处置时效。

然而，零散和隐晦的信息令开发者宛如在海量拼图碎片中寻觅，依靠耐心拼凑漏洞全貌。

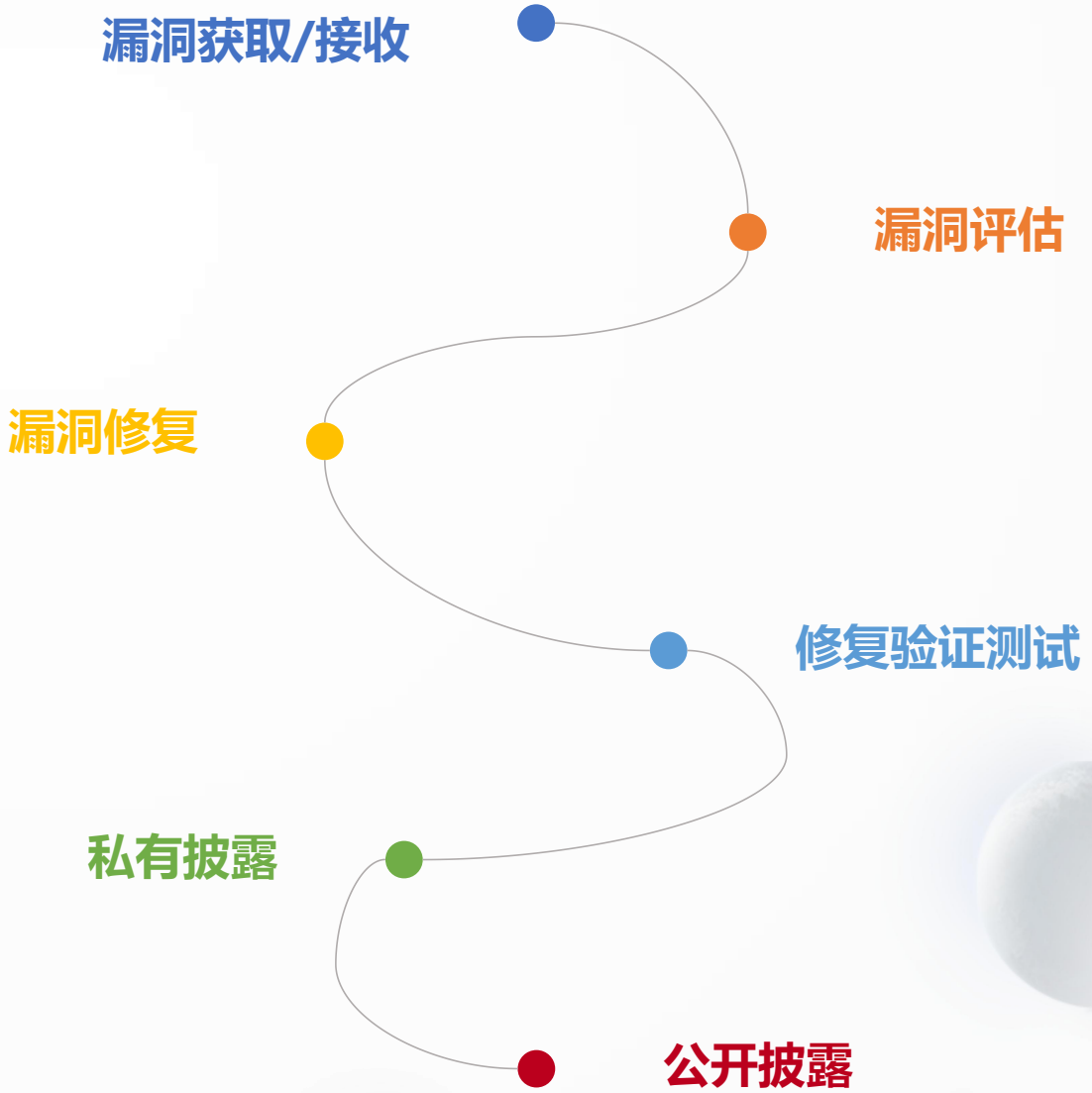
漏洞情报时效困境

现象和问题

漏洞处置速度慢

安全漏洞管理流程主要包含了漏洞接收、漏洞威胁评估、漏洞修复验证、私有披露与公开披露。其中漏洞评估需要漏洞细节、验证程序等关键知识，漏洞修复可能需要等待上游补丁。

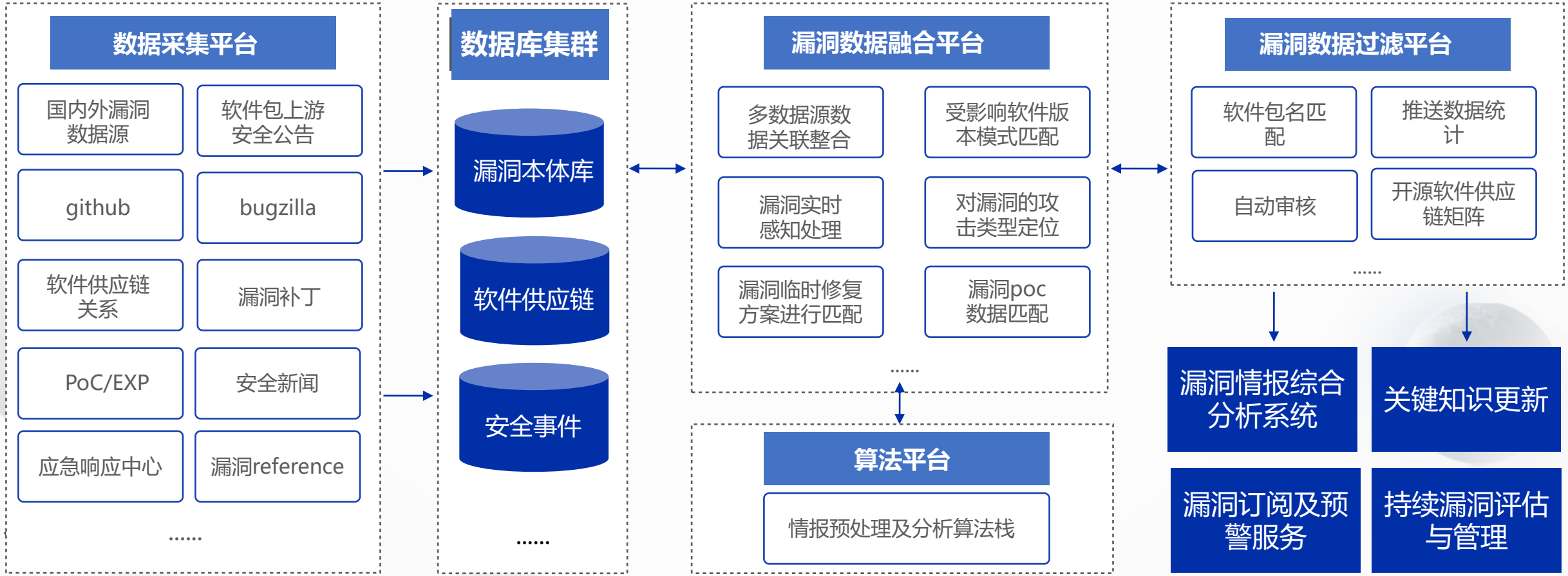
开源社区加快漏洞处置速度的方式包括建立合理高效的组织和流程，以及及时提供关键知识。



及时获取关键知识

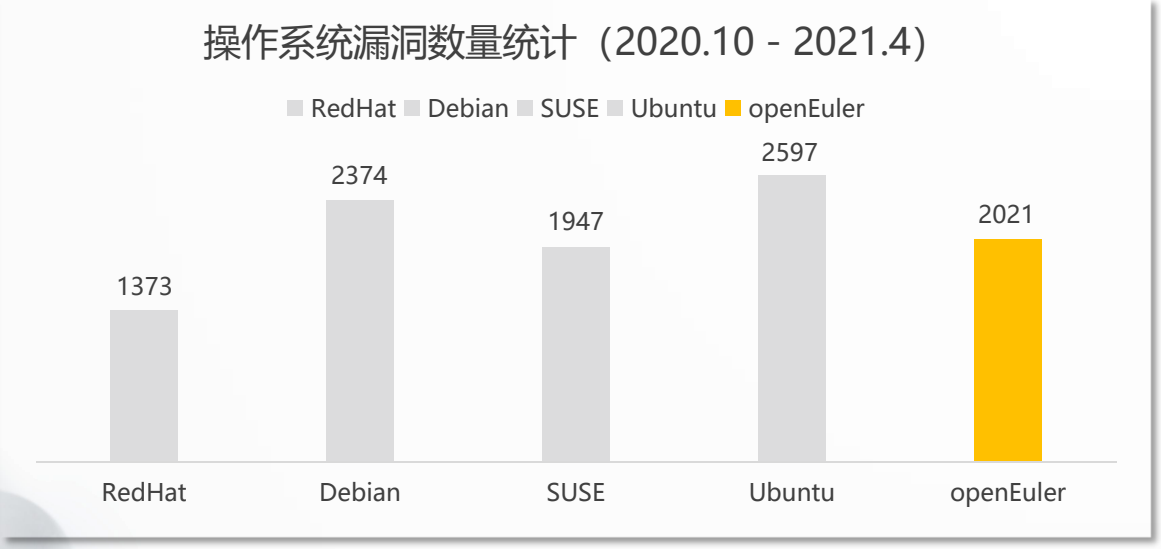
漏洞感知技术

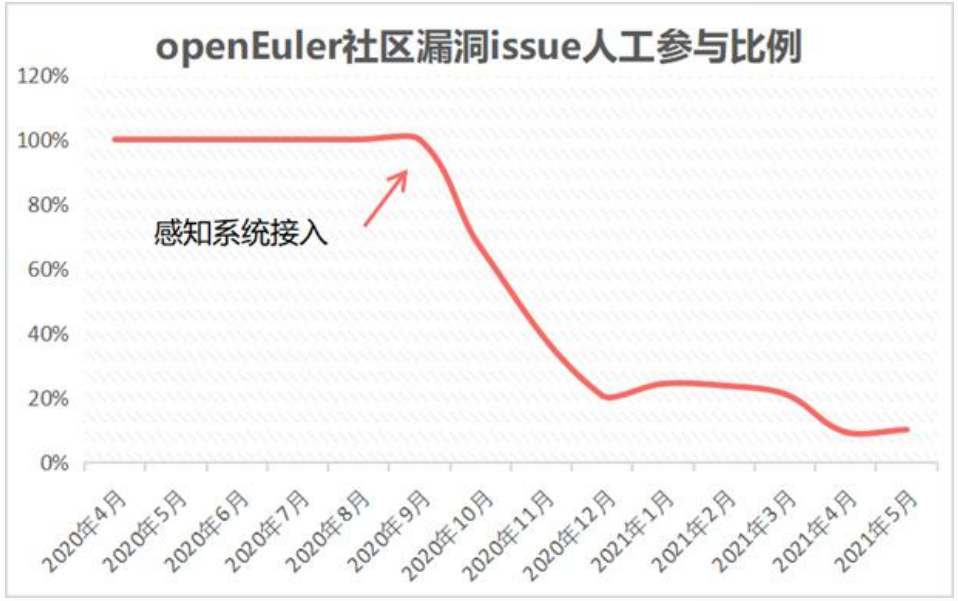
通过在全球范围进行实时的漏洞情报获取、汇总与分析，为开源社区实时提供相关漏洞情报与关键知识，从而**提升社区漏洞管理效率并降低人员与经验成本。**

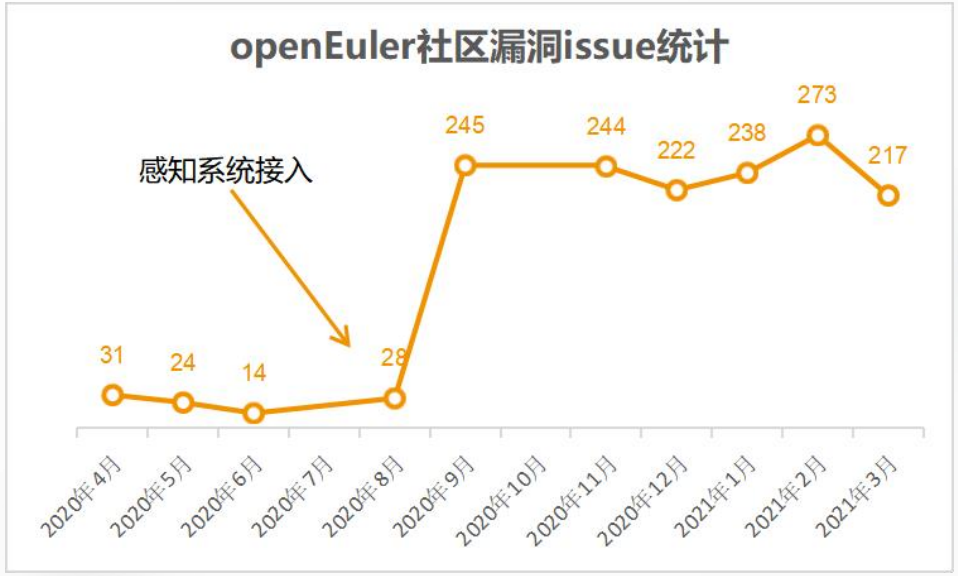


漏洞感知技术

2020年9月开始，openBrain为国内顶级开源社区建设人机协同的代码仓库漏洞感知体系，实现8000+开源组件的漏洞自动化识别、跟踪和管理。



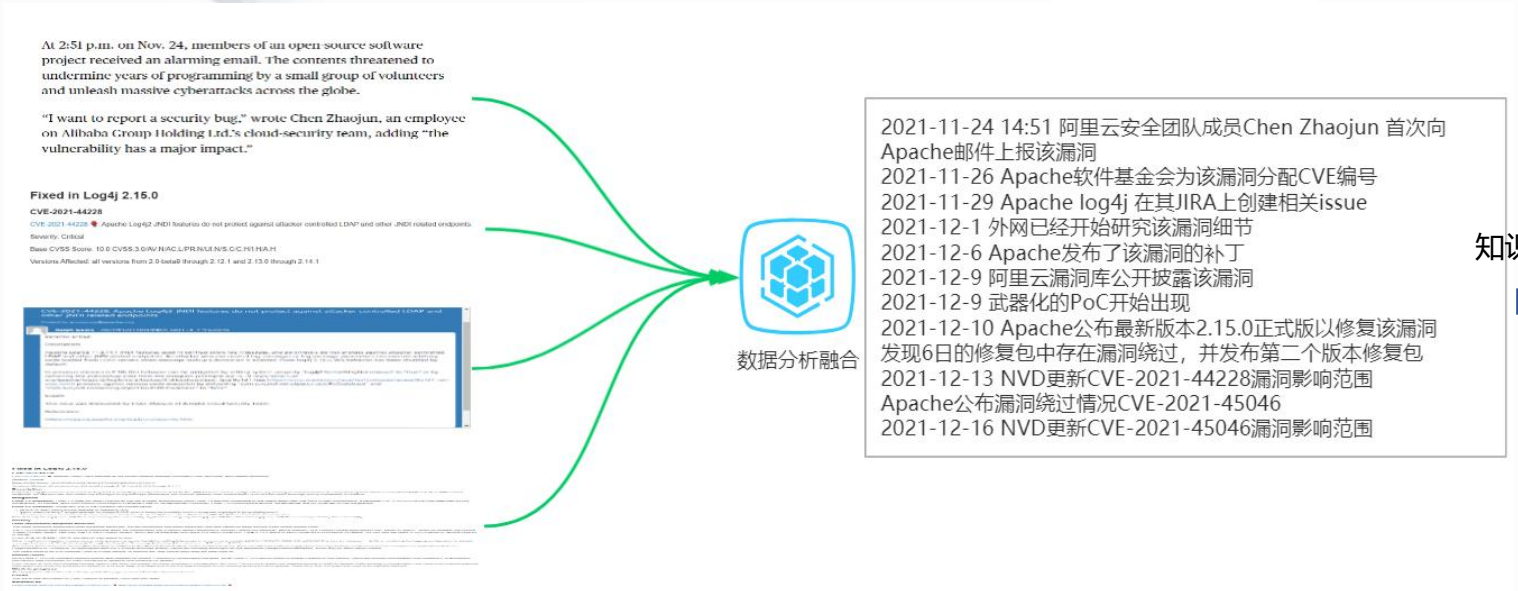




开源安全知识获取与处理

全球方位自动跟踪漏洞情报，通过高精度比对与持续看护降低成本并提升效率

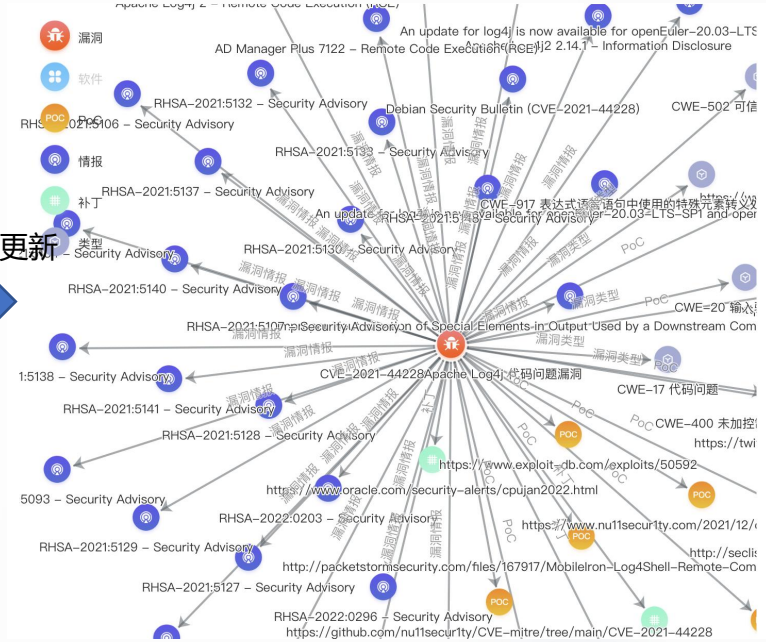
漏洞感知技术



数据分析融合

2021-11-24 14:51 阿里云安全团队成员Chen Zhaojun 首次向Apache邮件上报该漏洞
2021-11-26 Apache软件基金会为该漏洞分配CVE编号
2021-11-29 Apache log4j 在其JIRA上创建相关issue
2021-12-1 外网已经开始研究该漏洞细节
2021-12-6 Apache发布了该漏洞的补丁
2021-12-9 阿里云漏洞库公开披露该漏洞
2021-12-9 武器化的PoC开始出现
2021-12-10 Apache公布最新版本2.15.0正式版以修复该漏洞
发现6日的修复包中存在漏洞绕过，并发布第二个版本修复包
2021-12-13 NVD更新CVE-2021-44228漏洞影响范围
Apache公布漏洞绕过情况CVE-2021-45046
2021-12-16 NVD更新CVE-2021-45046漏洞影响范围

知识提取与更新



分散情报融合

多源异构数据整合并建立关系，提供完善漏洞视角，并对数据进行校验

及时获取关键知识

多源异构数据整合并建立关系，提供完善漏洞视角，并对数据进行校验

目录

技术概述

技术进展

应用扩展

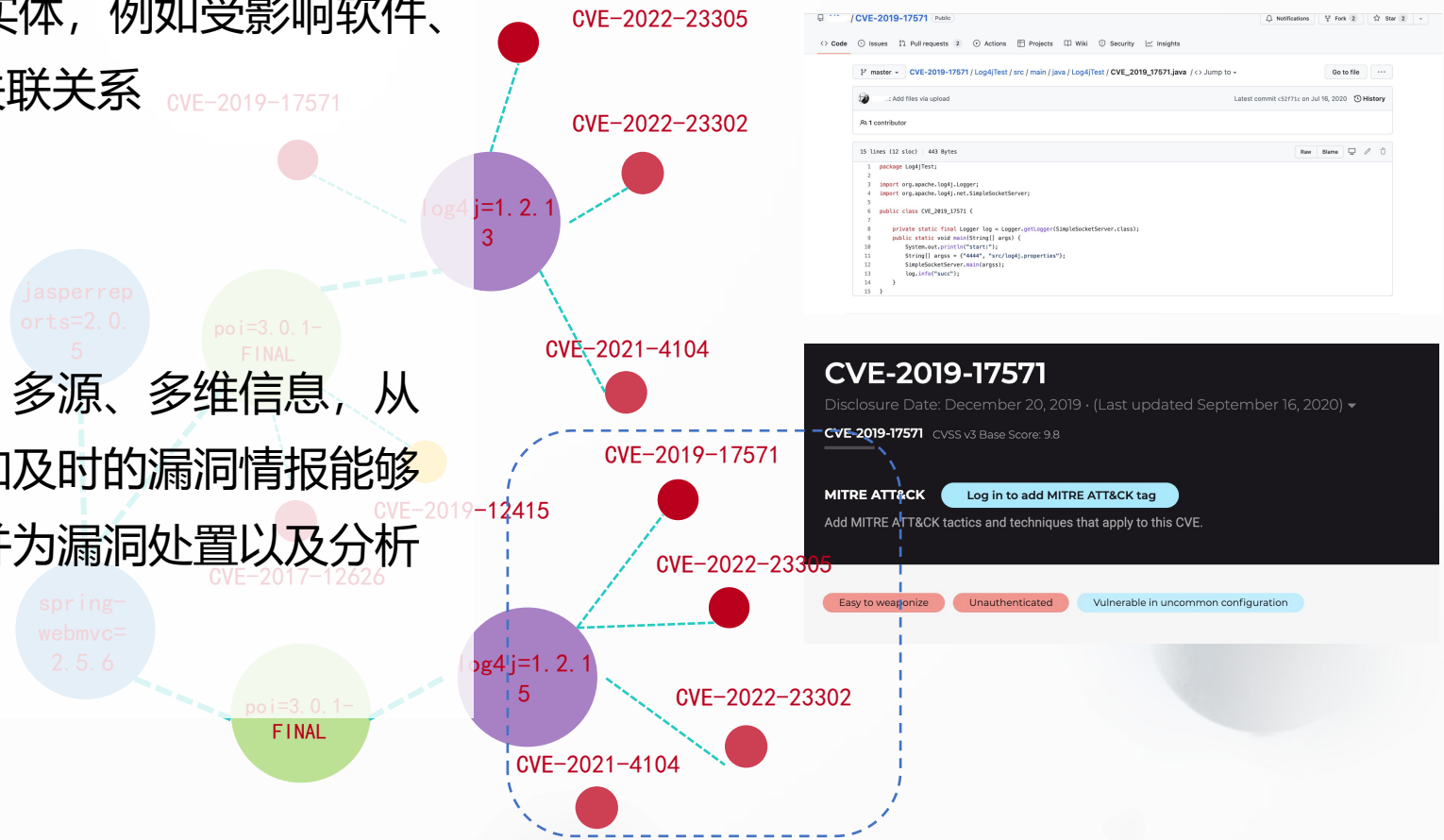
关键技术1：漏洞情报关联融合

Step1 构建统一的知识存储结构

Step2 对漏洞情报进行分类，提取关键实体，例如受影响软件、版本、补丁、PoC、安全事件等，形成关联关系

Step3 漏洞情报错误校正与信息补全

通过多源漏洞情报融合，有效整合大量、多源、多维信息，从而提升情报质量与及时性。同时，优质和及时的漏洞情报能够显著提升漏洞检测、评估等业务效果，并为漏洞处置以及分析工作提供有力支撑。



关键技术2：自动化供应链分析

挑战1 开源软件命名规则不统一

在不同漏洞情报源中，开源软件命名规则不统一，导致漏洞情报难以及时响应。

挑战2 同源开源软件代码差异

同源代码修改可能剪除或引入漏洞。

挑战3 大规模软件供应链分析

在大规模开源项目中，传统手段效率不足，准确性与全面性难以兼顾，难以满足时效性要求。

Step1 软件供应链溯源

通过在知识库中对开源软件上下游关系、依赖关系、包含关系等进行预构建和刻画。

Step2 开源漏洞传播模型

基于补丁比对的漏洞检测技术+软件供应链溯源，构建开源漏洞传播模型。

Step3 开源软件映射矩阵

维护开源软件映射矩阵，将不同数据源的软件归一化，实现快速的情报感知。

Anolis	upstream	Ubuntu	Fedora	Debian	other
-	docker	docker.io	docker	docker.io	。。。
apache-commons-compress	commons-compress	libcommons-compress-java	apache-commons-compress	libcommons-compress-java	。。。

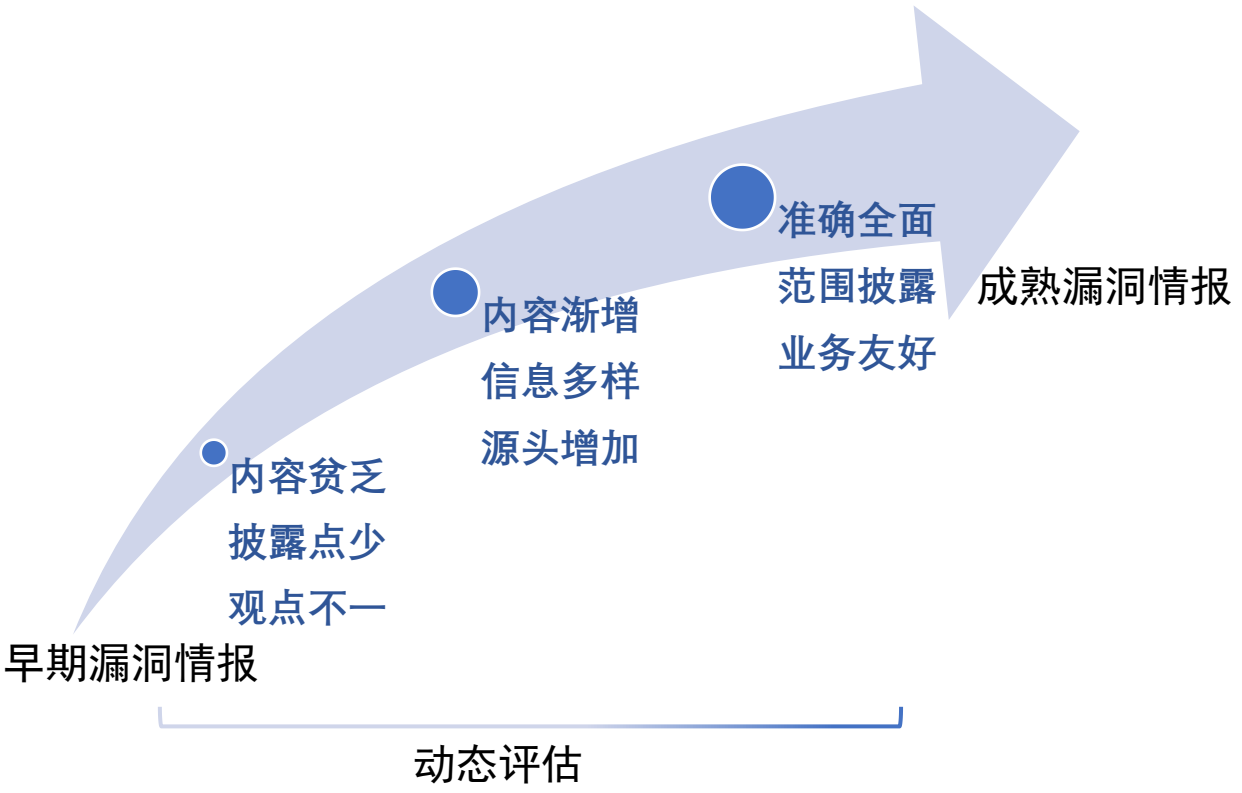
关键技术3：漏洞情报动态评级

挑战 漏洞情报质量 vs 时效性

早期出现的漏洞情报通常内容较少，不够准确。开源软件作为基础设施的核心要素，需要更早的漏洞情报并尽快进行响应，然而不准确的漏洞情报则会给社区带来额外负担。

方法 漏洞情报动态评级

根据不同情报内容和漏洞判定方式，实现漏洞情报动态评级系统，在每次情报更新后更新评级，并以此判断情报与开源项目的相关性。

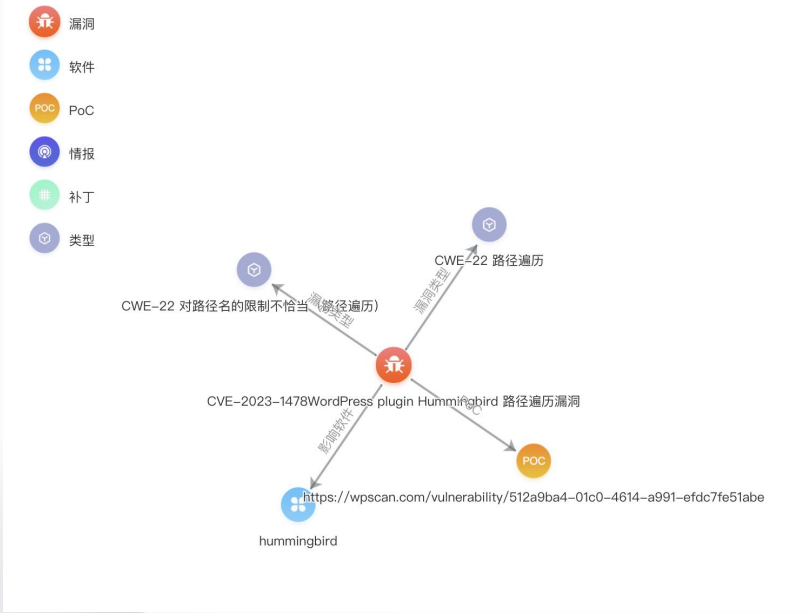


漏洞情报时效困境

多维度情报融合与置信度动态评级

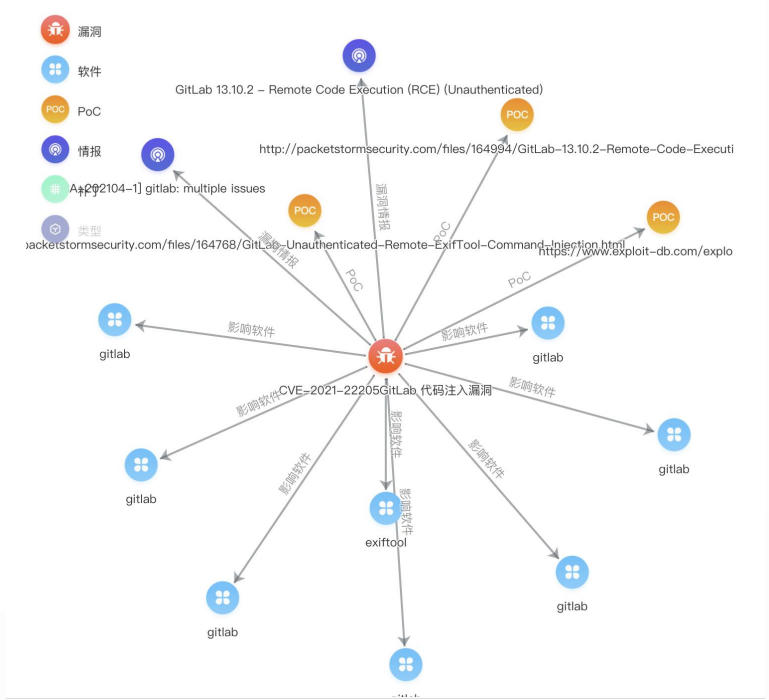
关键技术4：动态处置优先级评估

时刻跟踪漏洞在外网的讨论热度、舆情、武器化潜力、攻击事件等多个维度，综合评估漏洞处置优先级，帮助社区漏洞修复小组识别漏洞外部威胁态势，更快修复关键漏洞。



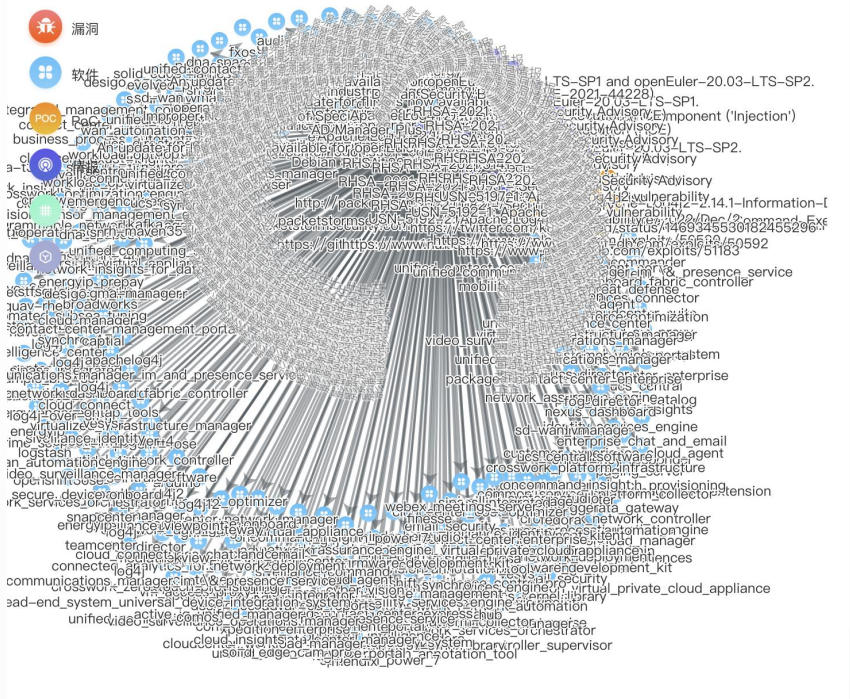
紧急漏洞

示例：CVE-2023-1478，评分9.8，WordPress plugin Hummingbird 路径遍历漏洞



武器化漏洞

示例：CVE-2021-22205，评分10，GitLab 代码注入漏洞

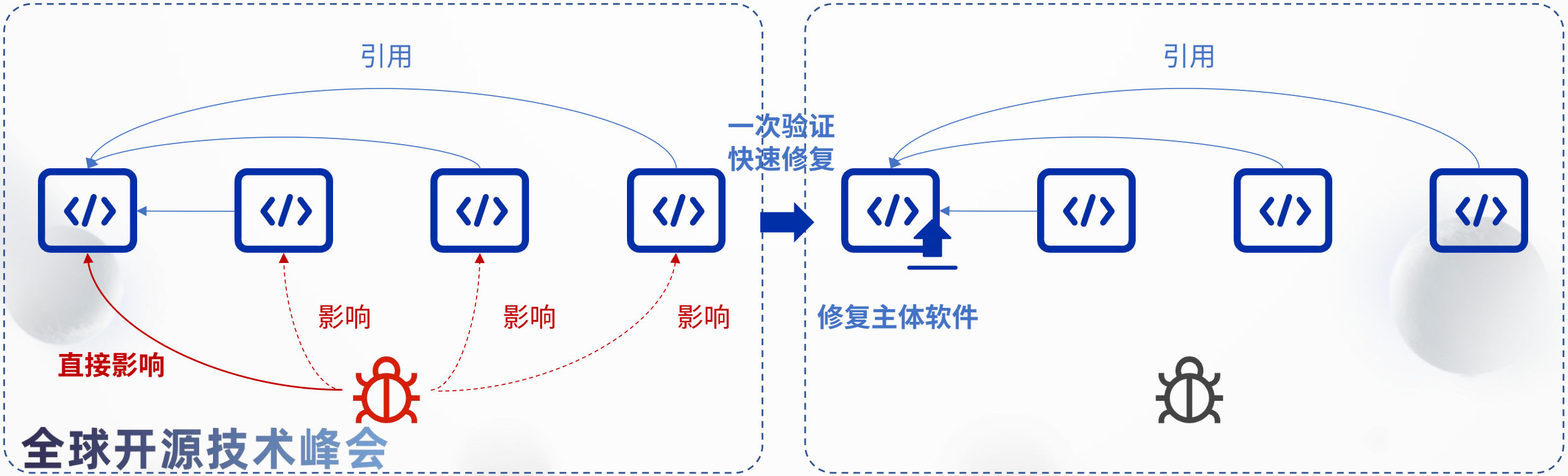


“核弹级”漏洞

示例：CVE-2021-44228，评分10，log4shell漏洞

关键技术5：主体软件识别

在操作系统中，漏洞的影响范围可能涉及多款软件。但其中部分软件可能是由于引用了那些漏洞直接影响的软件，从而受到影响。我们将那些漏洞直接影响的软件成为**主体软件**。为此，识别和修复漏洞影响的主体软件能够快速消除漏洞影响范围，提升修复效率。



关键技术6：Standard Vulnerability Schema

OpenBrain提供实时漏洞情报数据汇总，并形成漏洞情报共享接口。

Standard Vulnerability Schema涵盖数百个漏洞情报源，实时更新结构化漏洞情报，面向工具和业务进行情报共享。

- 开源漏洞感知系统
- 漏洞优先级
- 软件成分分析（SCA）
- 漏洞验证测试
- 开源漏洞管理系统
- 漏洞修复
- 漏洞库与情报共享
- 供应链风险

……


```
{
  "_id": ObjectId("63c6f9f52c9c925d8f833d6c"),
  "ids": "CVE-2022-46285",
  "cveNum": "CVE-2022-46285",
  "cvePackName": [
    "libxpm"
  ],
  "packName": [
    "libXpm==3.5.13"
  ],
  "packNames": [
    "libXpm"
  ],
  "description": {
    "en": "A flaw was found in libXpm. This issue occurs when parsing a file with a comment not closed; the end-of-file condition will not be detected, leading to an infinite loop and resulting in a Denial of Service in the application linked to the library.",
```


Standard Vulnerability Schema 示例

阶段成果

GOTC

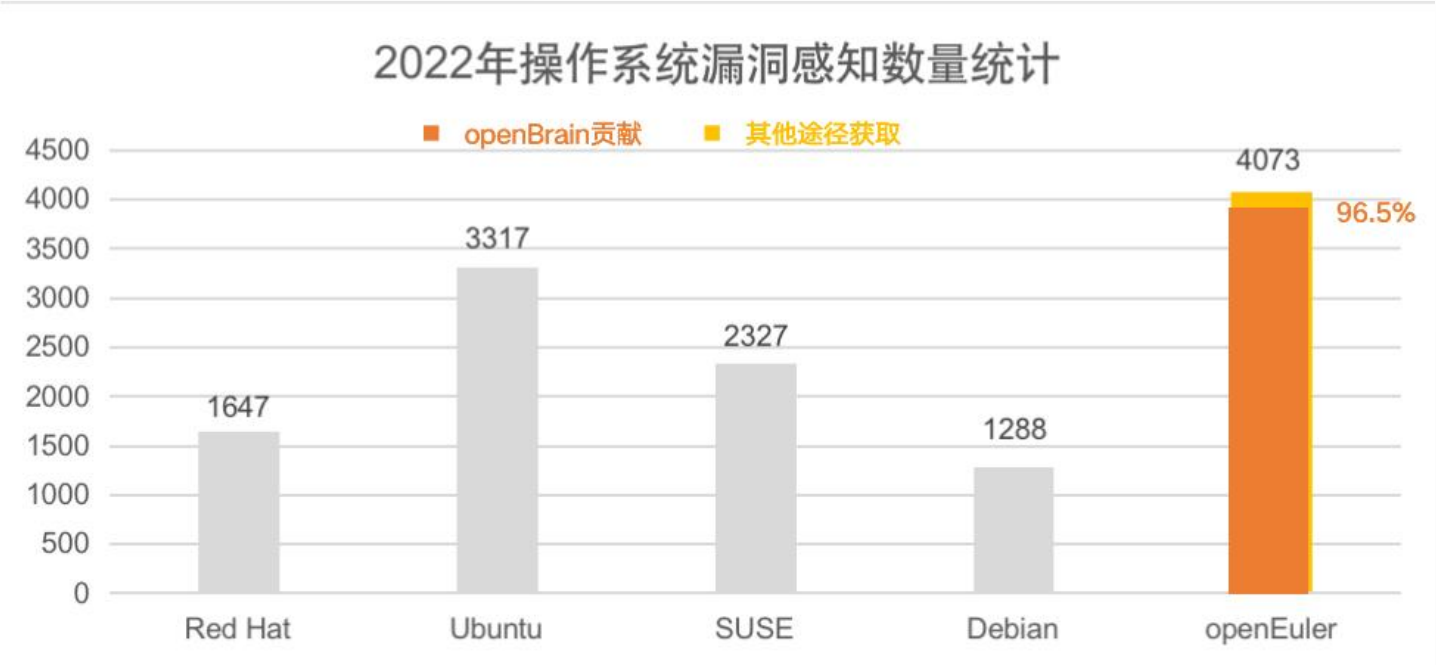
2020.10-2022.10

26.5万	7120	95%	1119	23 Days
漏洞总数	创建漏洞ISSUE	漏洞贡献	早于NVD披露	提前感知时长

阶段成果

2022年，openBrain推送有效漏洞数据达到总漏洞数**96.5%**，漏洞感知数量超过国际顶级操作系统。实现对大规模开源组件自动化漏洞管理，对超过**8000款**开源组件多版本进行实时漏洞情报监测与分析，汇总包括验证程序、修复方案在内的多类情报，缩短安全漏洞暴漏窗口期。

下阶段，openBrain将聚焦进一步提升时效性，并降低社区漏洞处置难度，提升漏洞处置速度。



99%
最高准确率

- 2022年9月和10月，openBrain达到最高准确率。

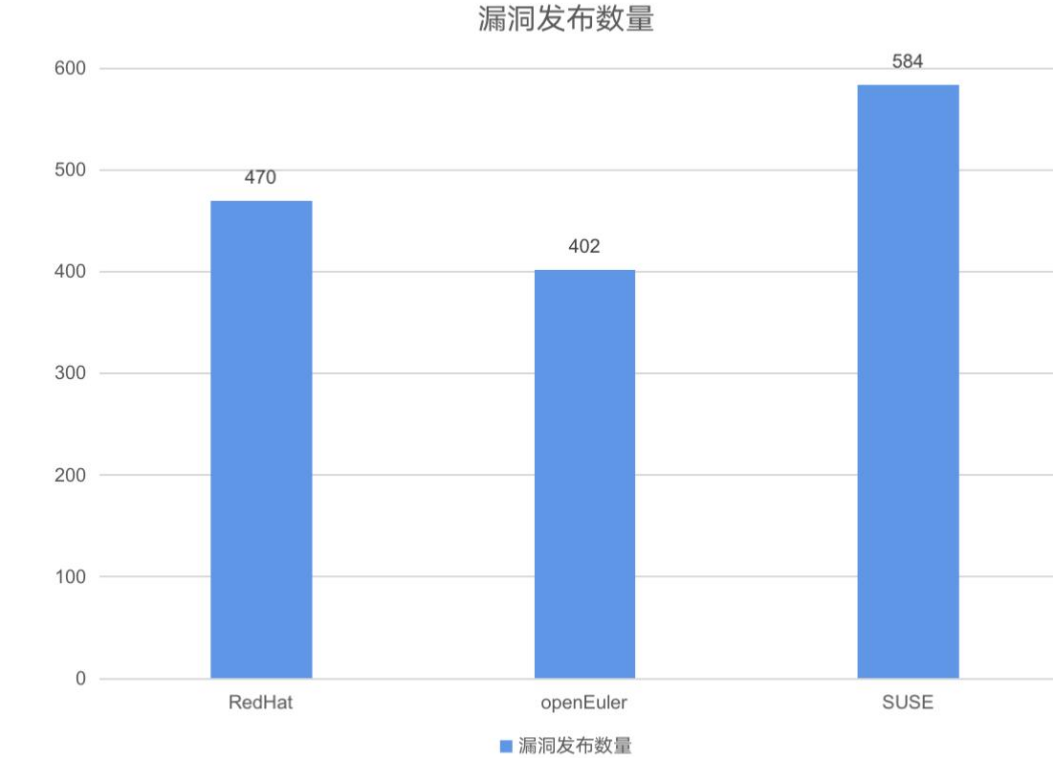
46天
时效性

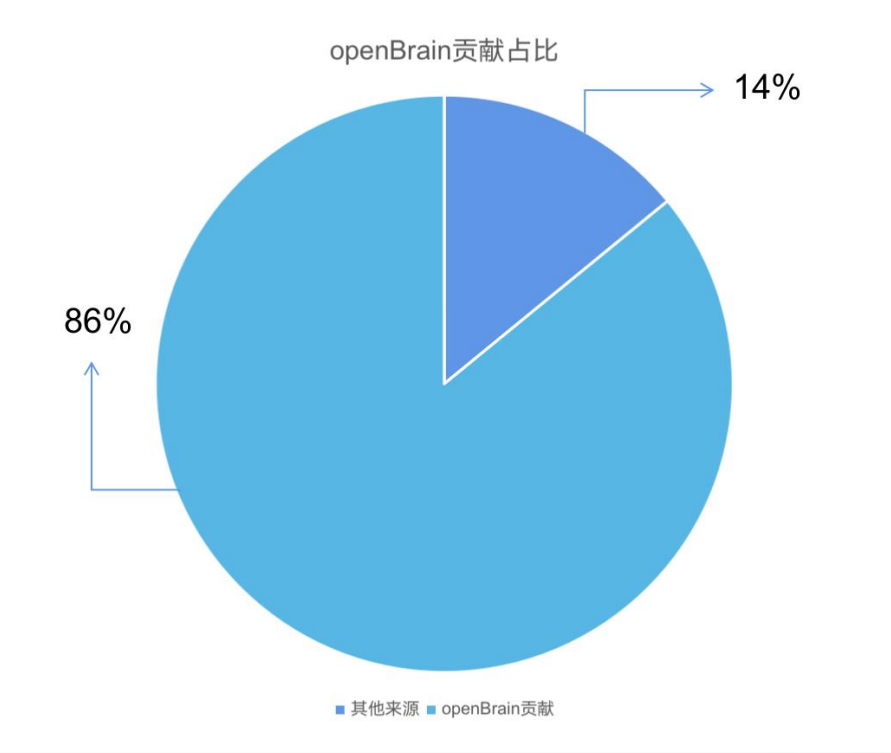
- 2022年里，openBrain最早比NVD提前46天完成漏洞上报。

阶段成果

2023年1月至4月17日，openEuler发布安全公告402个，与国际顶级OS社区保持同步。

其中openBrain贡献占比**86%**，总体准确率**96%**，近**59%**漏洞ISSUE提交时间早于美国国家安全漏洞库（NVD）。

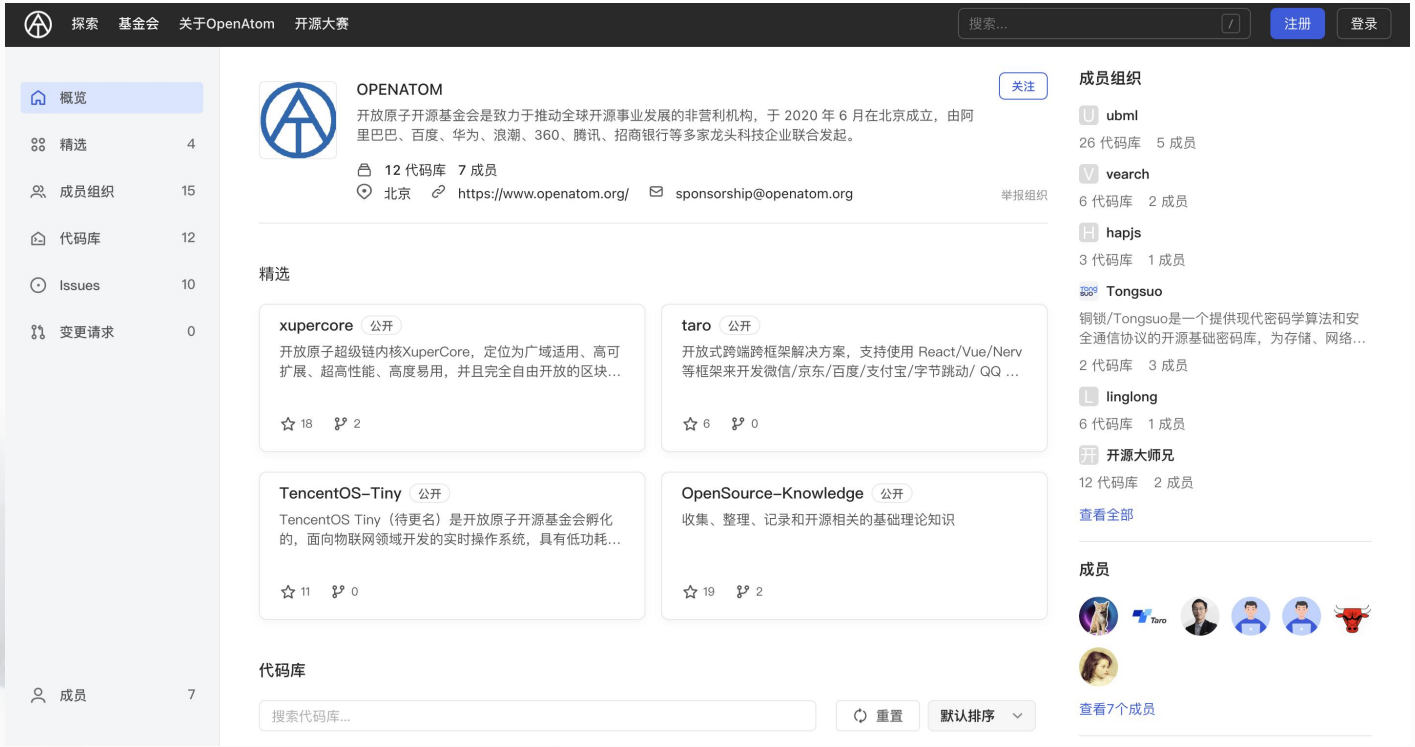


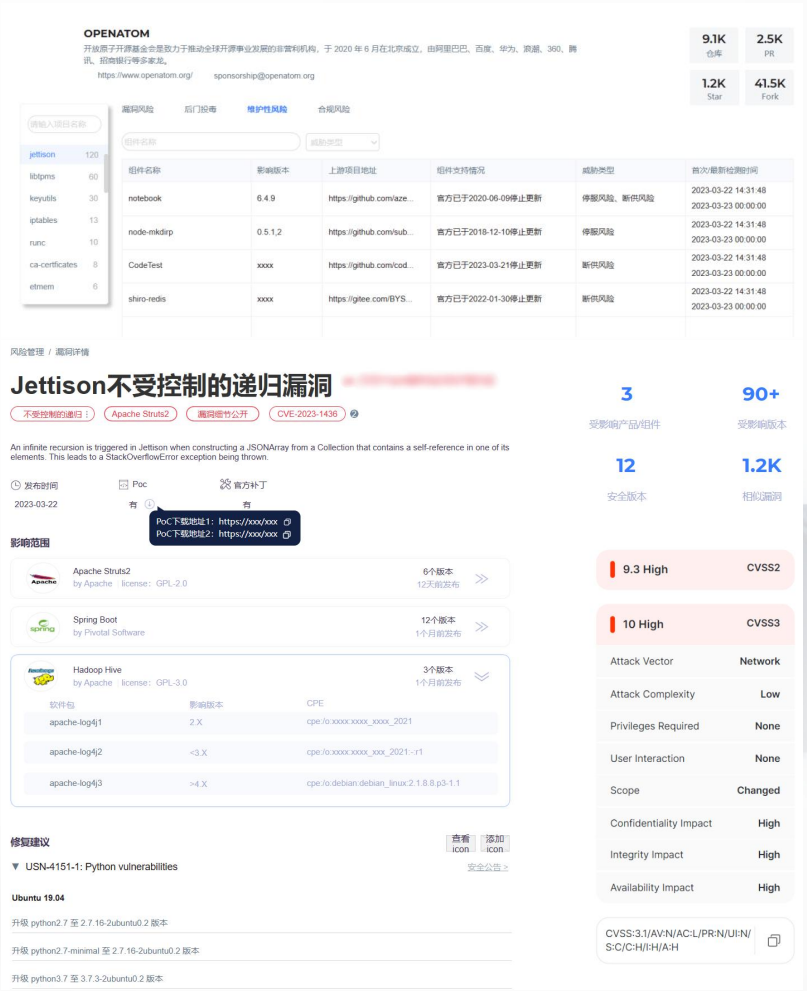


目录

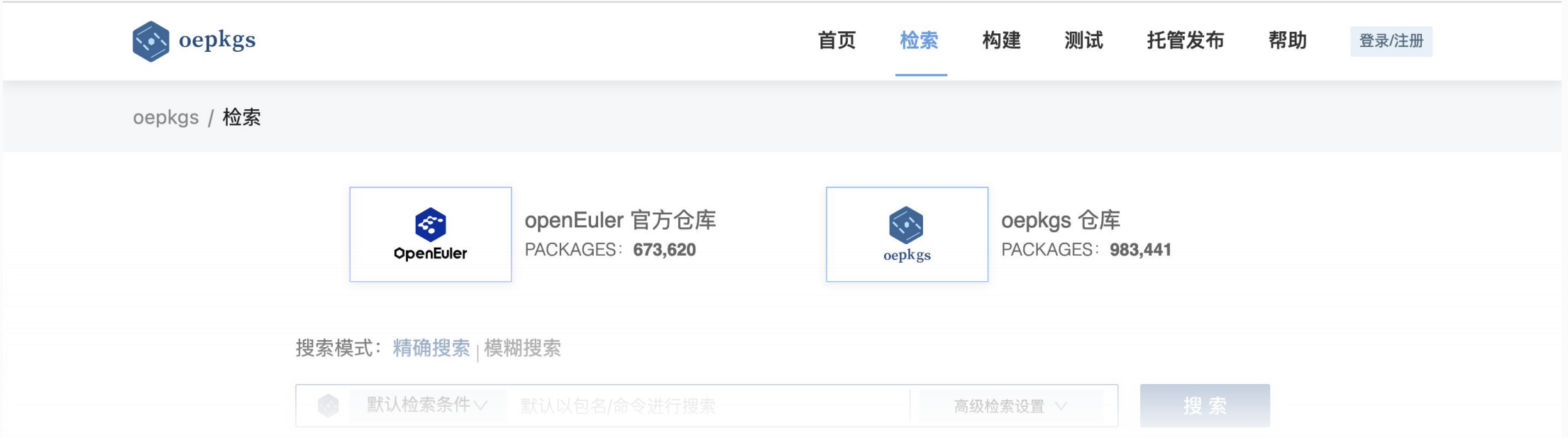
基金会开源漏洞感知

openBrain接入开放原子开源基金会AtomGit，面向基金会旗下项目提供开源软件供应链风险监测与漏洞感知能力。





oepkgs漏洞感知

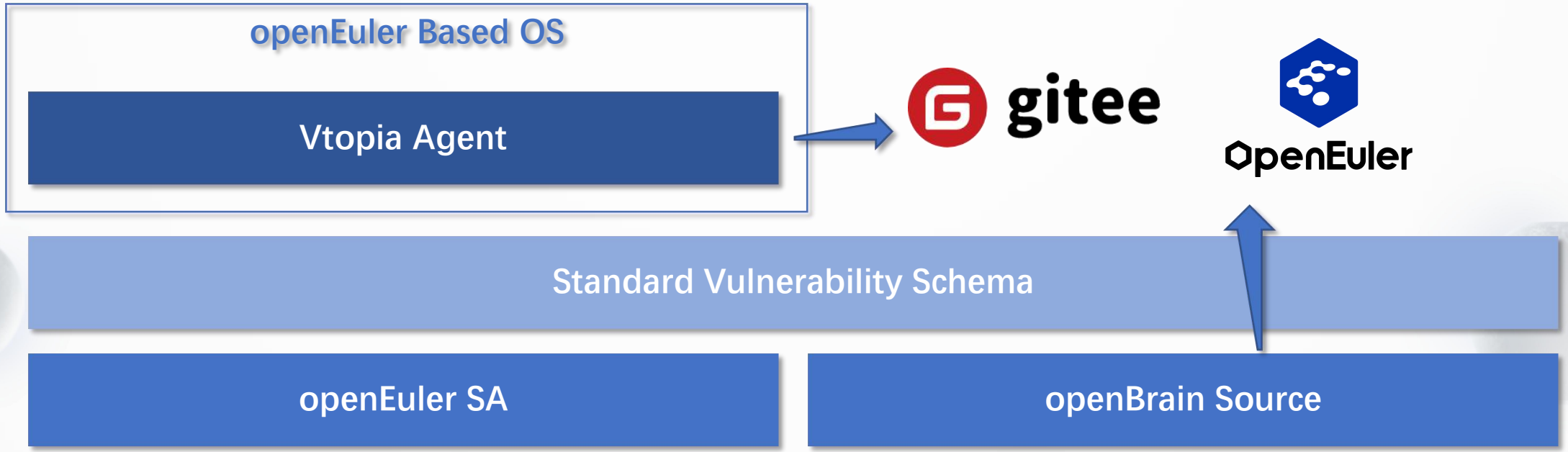


oepkgs 全称为开放软件包服务（Open External Packages Service），是一个为openEuler以及其他Linux发行版提供软件包服务的第三方社区。openBrain能力引入oepkgs，实现oepkgs托管软件包的常态化漏洞感知能力，提供漏洞感知、动态优先级评估、关键漏洞预警、关键知识推送等服务。

Vtopia Agent 运行时供应链安全

将openEuler安全能力从开源社区延伸至各类最终用户，打通openEuler供应链安全链路，实现从开源代码到运行时的数据对齐与能力共享。

启动开源Vtopia Agent项目捐赠，为openEuler生态提供运行时漏洞监测与修复能力。



GOTC

THANKS

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE