



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。



技术概述



技术进展



应用扩展





技术概述



技术进展



应用扩展

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

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

Configuration	Link
Configuration 1	Link
Configuration 2	Link
Configuration 3	Link
Configuration 4	Link

CVE-2019-17571

Disclosure Date: December 20, 2019 · (Last updated September 16, 2020) ▾

CVE-2019-17571 CVSS v3 Base Score: 9.8

MITRE ATT&CK

Log in to add MITRE ATT&CK tag

Add MITRE ATT&CK tactics and techniques that apply to this CVE.

Easy to weaponize

Unauthenticated

Vulnerable in uncommon configuration

September 15, 2021 · 8 min read

Analyzing attacks that exploit the CVE-2021-40444 MSHTML vulnerability

Microsoft Defender Threat Intelligence
Microsoft Threat Intelligence Center (MSTIC)

Share

In August, Microsoft Threat Intelligence Center (MSTIC) identified a small number of attacks (less than 10) that attempted to exploit a remote code execution vulnerability in MSHTML using specially crafted Microsoft Office documents. These attacks used the vulnerability, tracked as [CVE-2021-40444](#), as part of an initial access campaign that distributed custom Cobalt Strike Beacon loaders. These loaders

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

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。

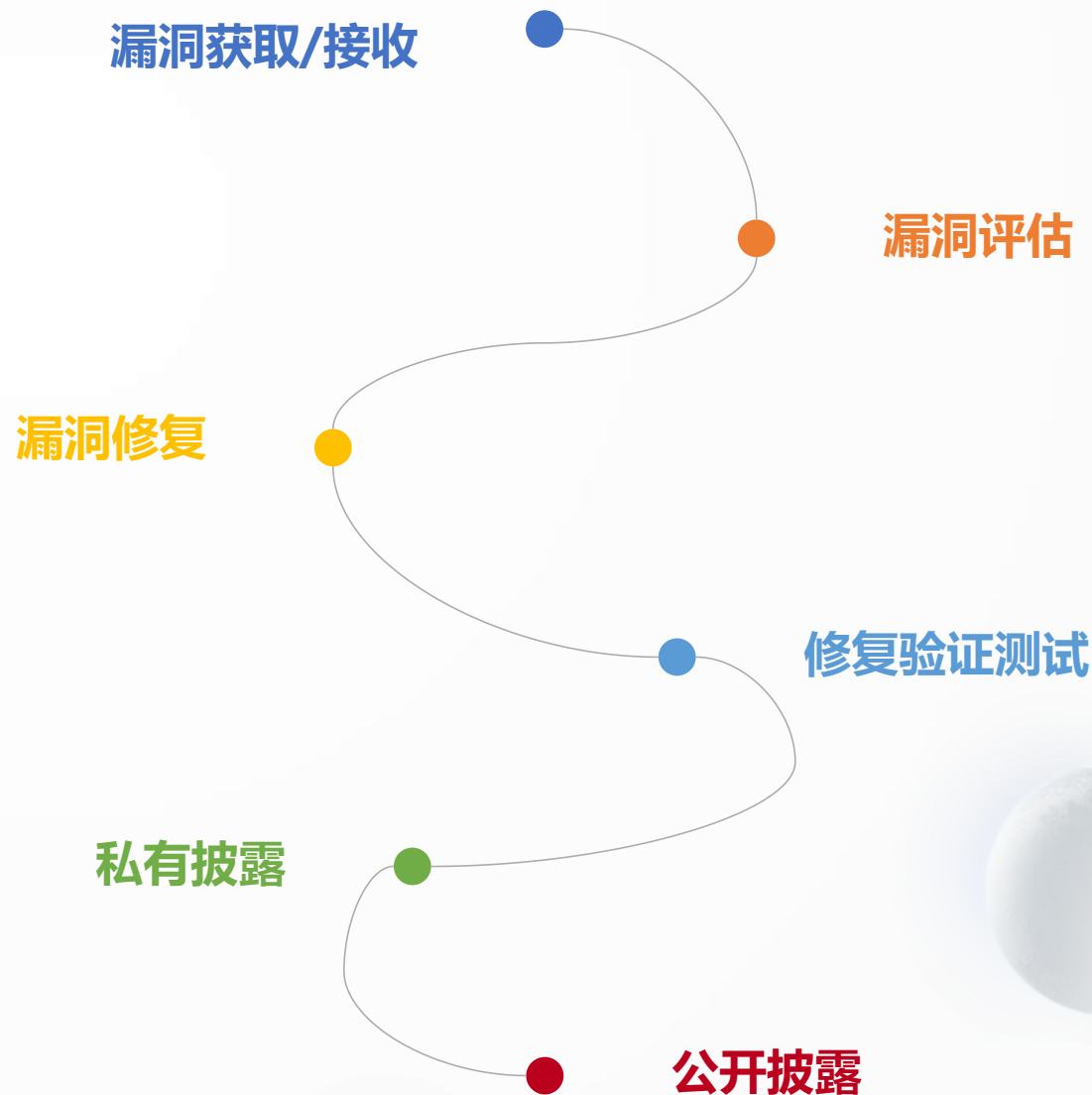
开源社区加快漏洞处置速度的方式包括建立合理高效的组织和流程，以及及时提供关键知识。



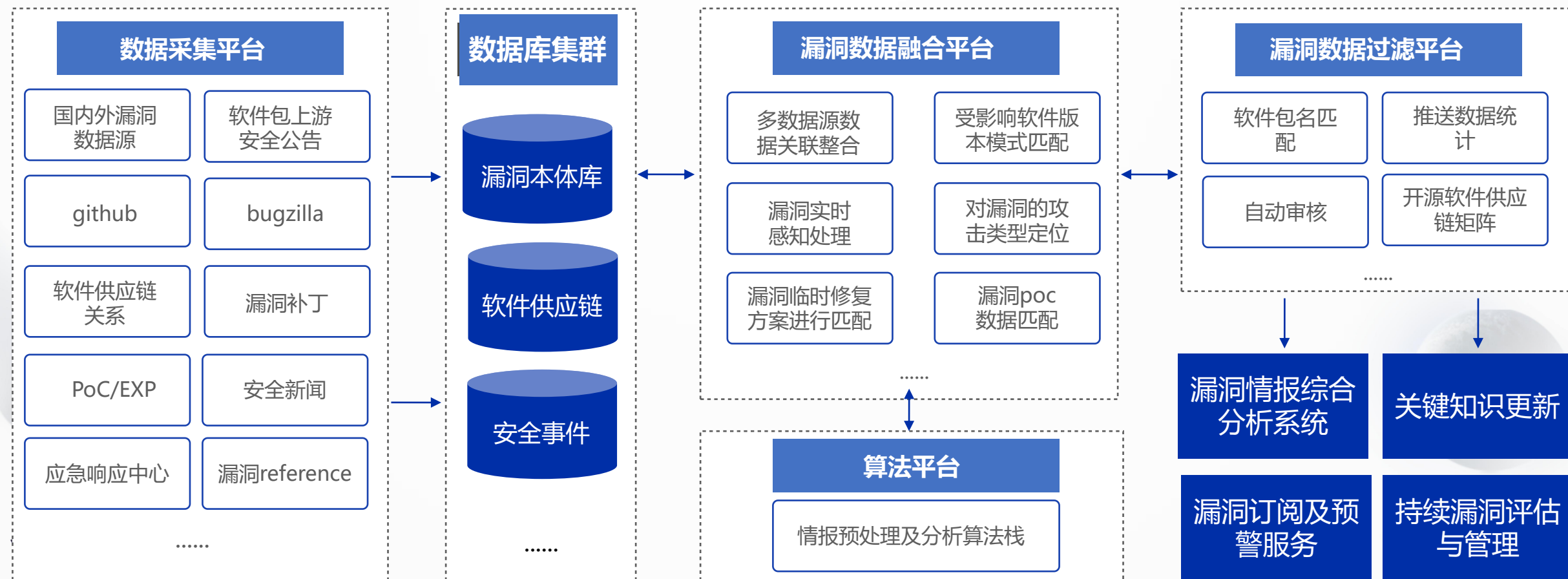
及时获取关键知识

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

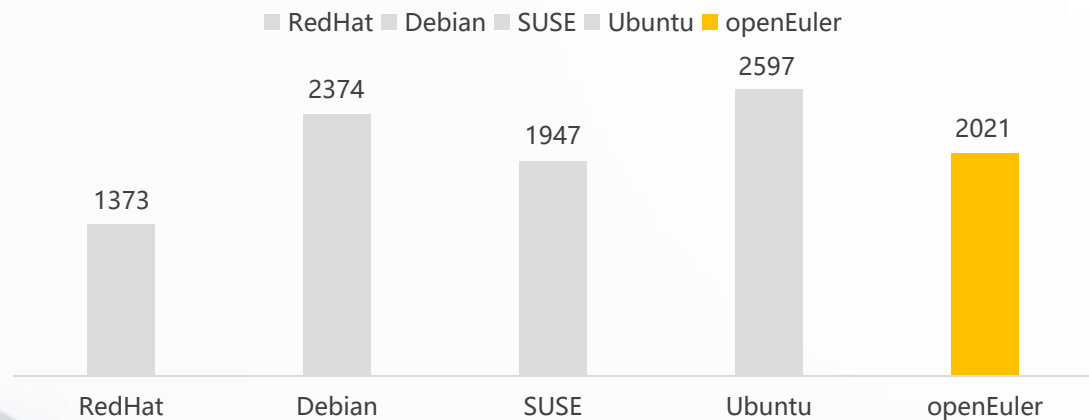


通过在全球范围进行实时的漏洞情报获取、汇总与分析，为开源社区实时提供相关漏洞情报与关键知识，从而**提升社区漏洞管理效率并降低人员与经验成本**。



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。

操作系统漏洞数量统计 (2020.10 - 2021.4)

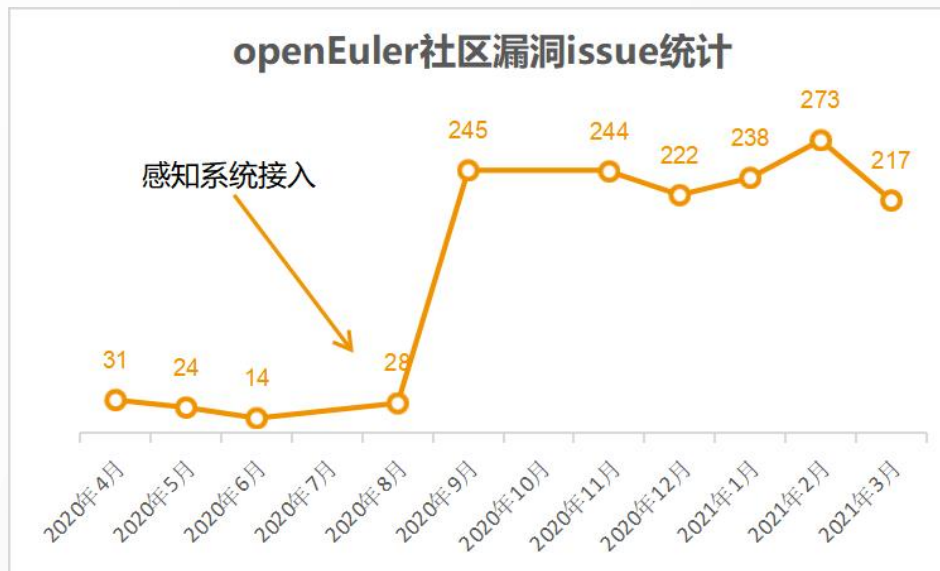
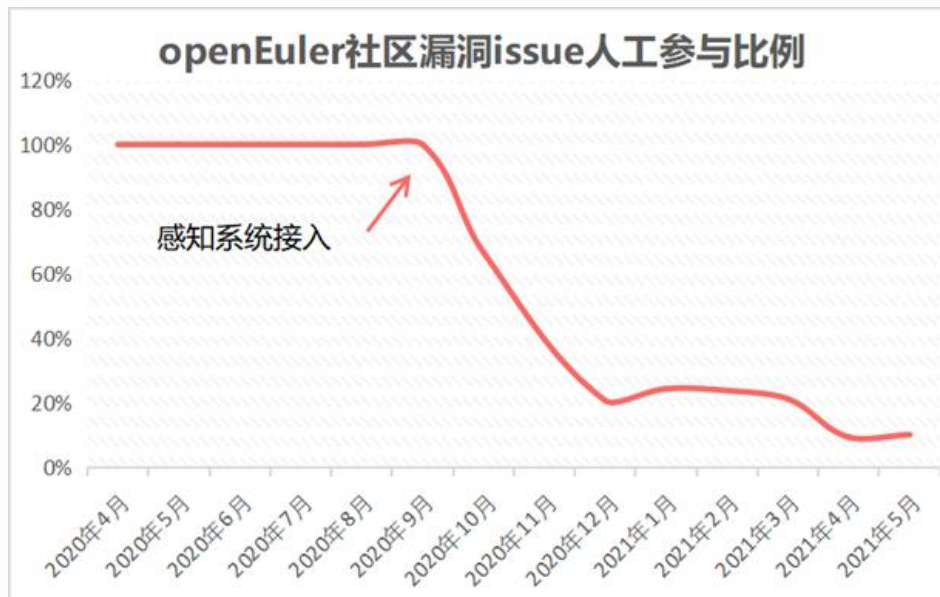


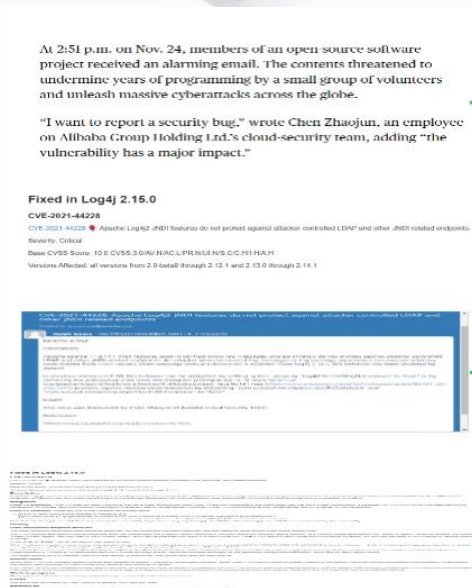
开源安全知识获取与处理

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

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

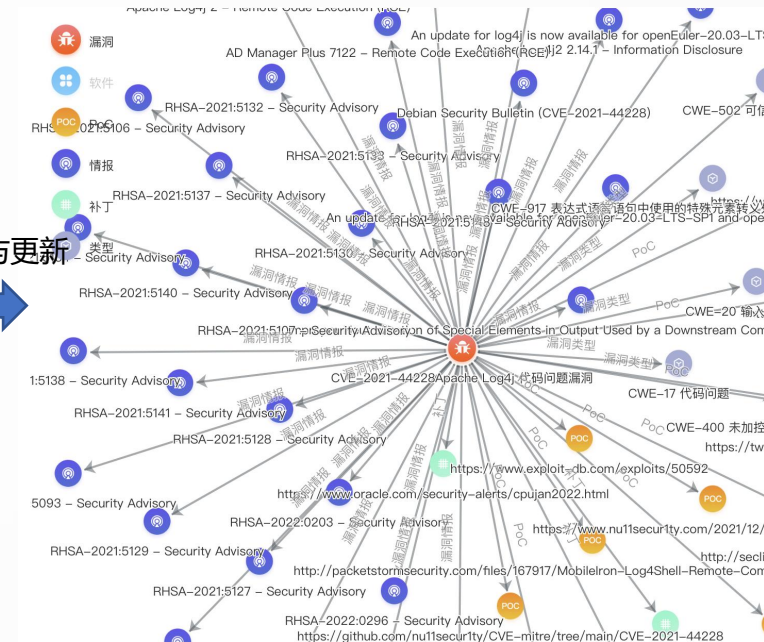




数据分析融合

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



技术概述



技术进展



应用扩展

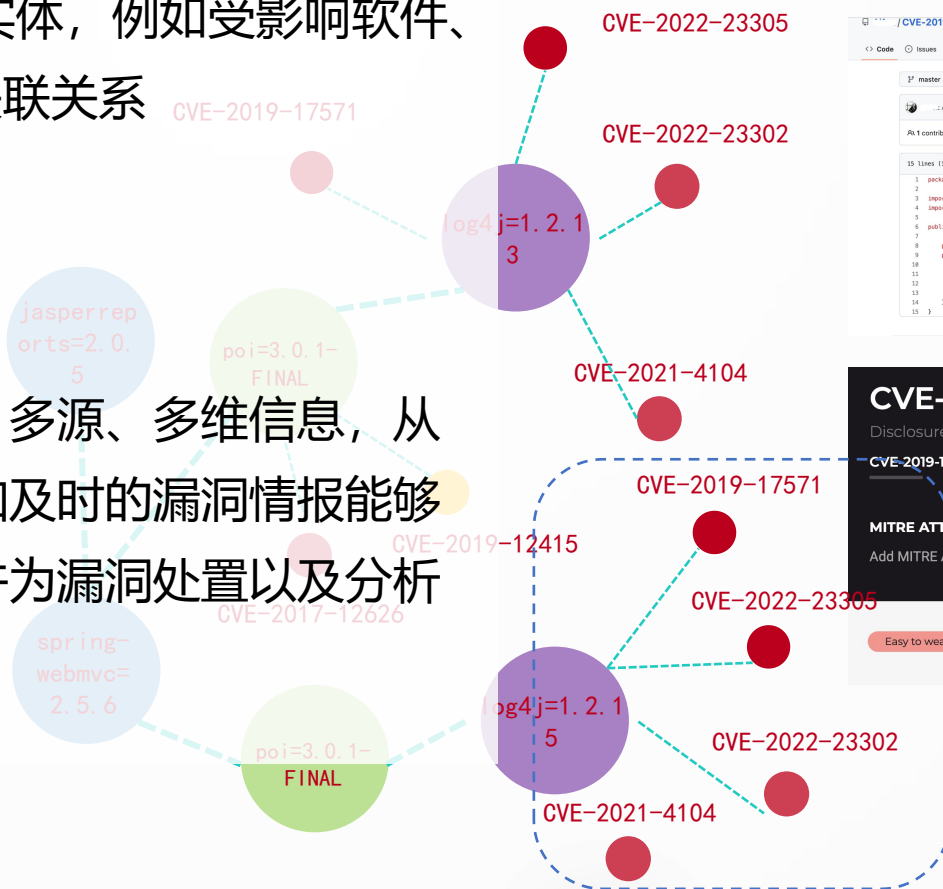
关键技术1：漏洞情报关联融合

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。



```
1 package Log4jTest;
2
3 import org.apache.log4j.Logger;
4 import org.apache.log4j.net.SocketServer;
5
6 public class CVE_2019_17571 {
7
8     private static final Logger log = Logger.getLogger(SocketServer.class);
9     public static void main(String[] args) {
10         System.out.println("Start");
11         String[] args = {"0.0.0.0", "8080", "org.apache.log4j.properties"};
12         SocketServer.main(args);
13         log.info("Success");
14     }
15 }
```

CVE-2019-17571
Disclosure Date: December 20, 2019 - (Last updated September 16, 2020)
CVSS v3 Base Score: 9.8
MITRE ATT&CK Log in to add MITRE ATT&CK tag
Add MITRE ATT&CK tactics and techniques that apply to this CVE.
Easy to weaponize Unauthenticated Vulnerable in uncommon configuration

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

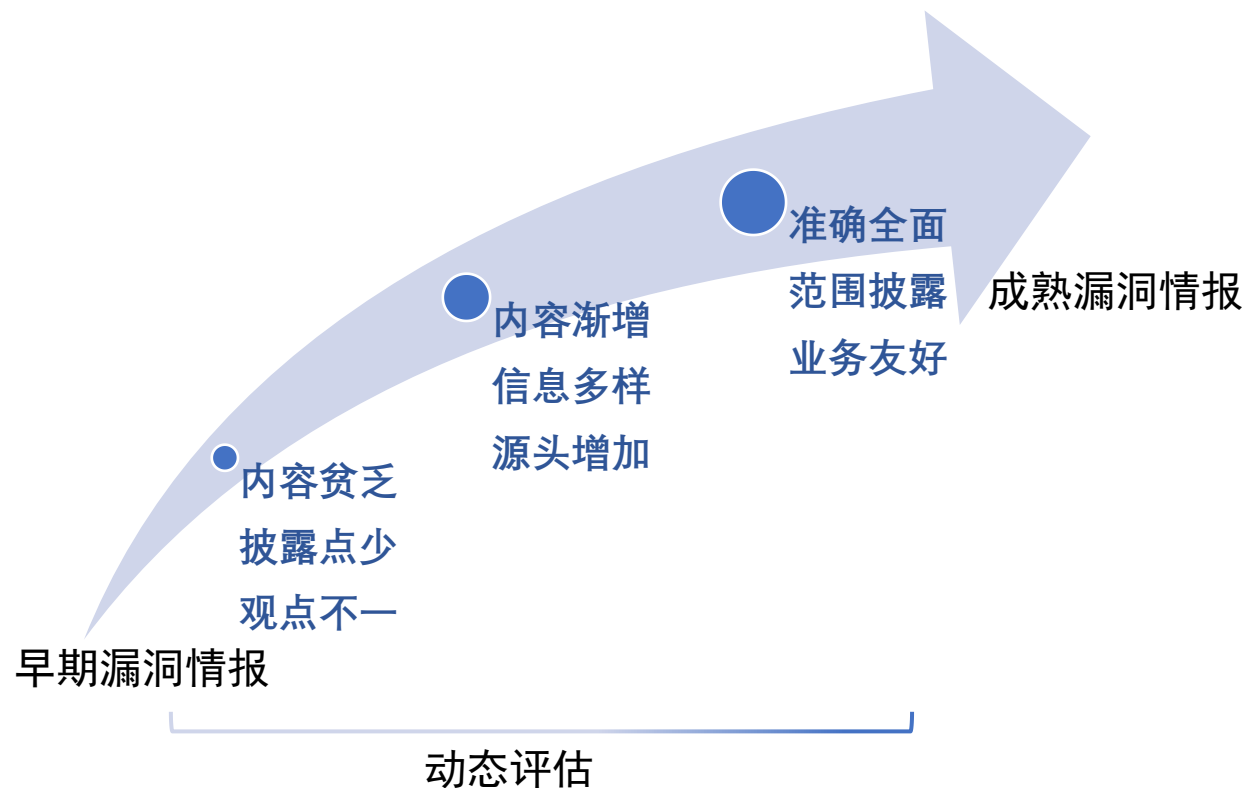
早期出现的漏洞情报通常内容较少，不够准确。开源软件作为基础设施的核心要素，需要更早的漏洞情报并尽快进行响应，然而不准确的漏洞情报则会给社区带来额外负担。

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。

全球开源技术峰会

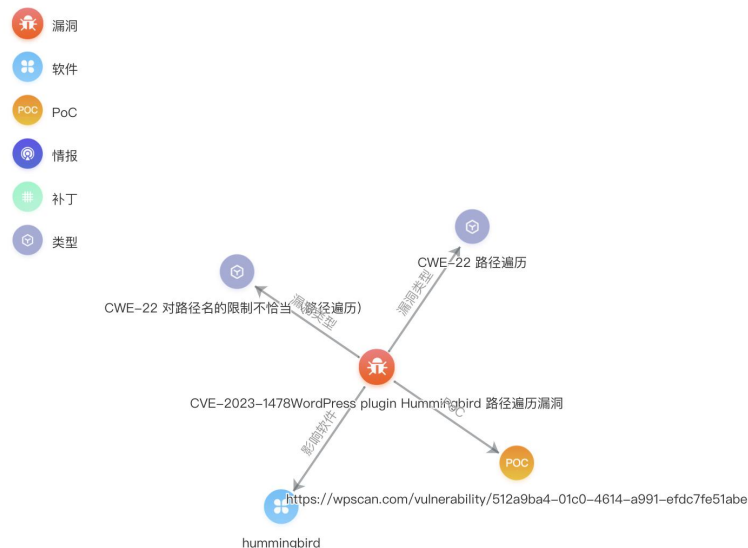
THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE



漏洞情报时效困境

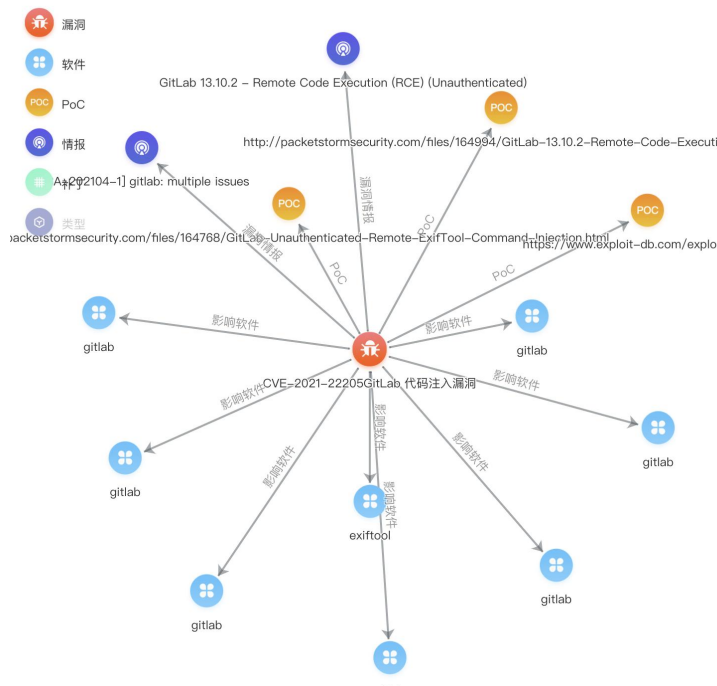
多维度情报融合与置信度动态评级

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。



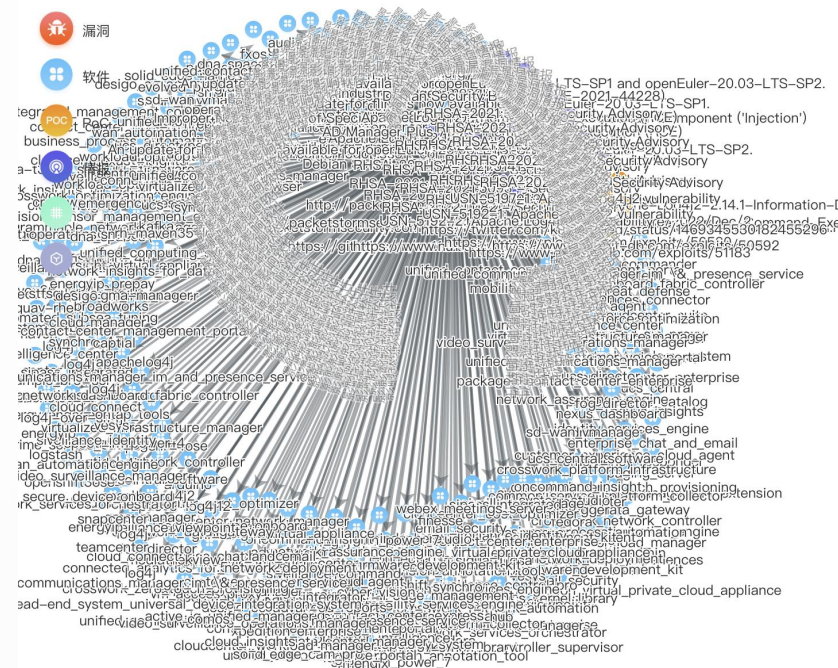
紧急漏洞

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

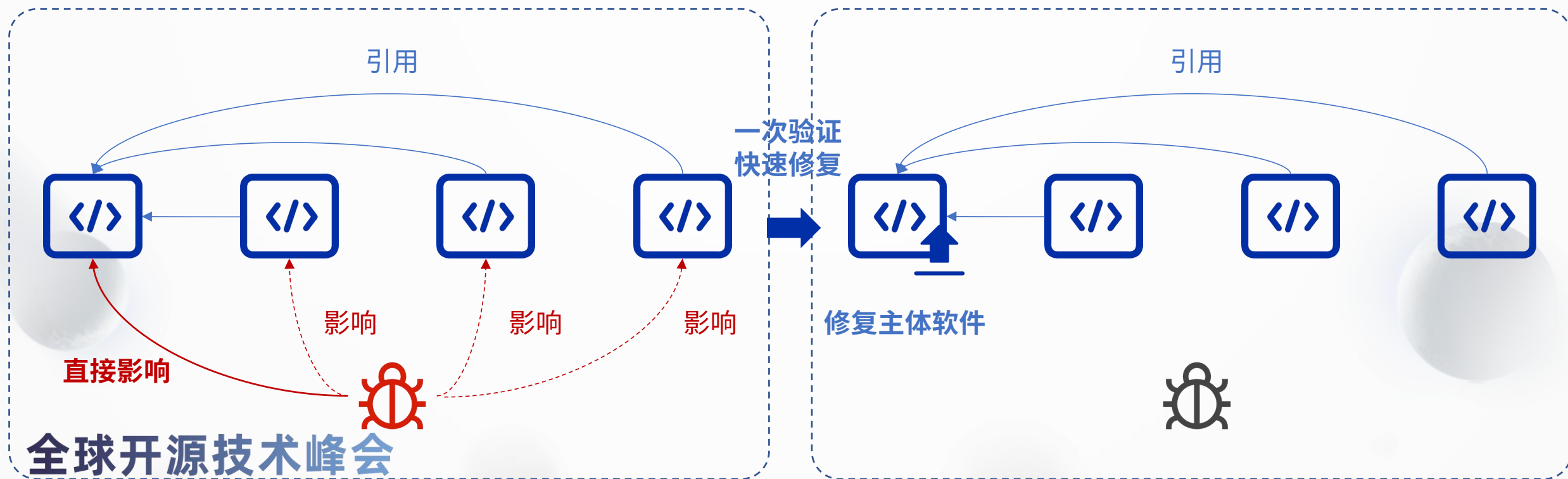


“核弹级”漏洞

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

.....

全球开源技术峰会

THE GLOBAL OPENSOURCE TECHNOLOGY CONFERENCE

```
{
  "_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

2020.10-2022.10

26.5万
漏洞总数

7120
创建漏洞ISSUE

95%
漏洞贡献

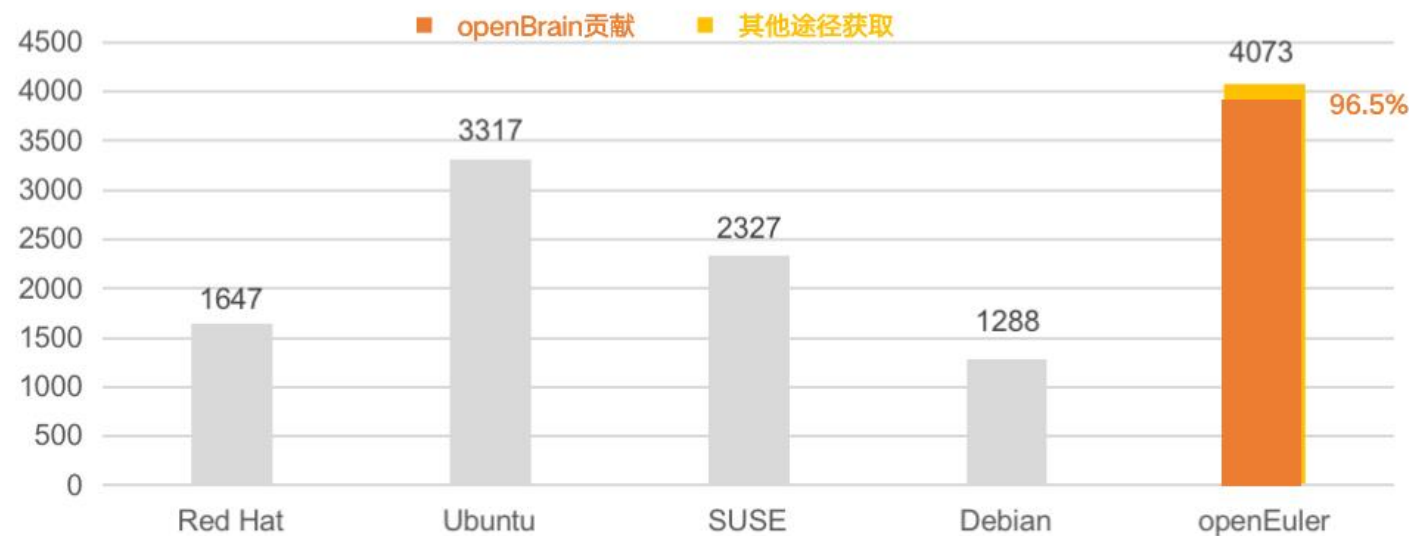
1119
早于NVD披露

23 Days
提前感知时长

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。

2022年操作系统漏洞感知数量统计



99%

最高准确率

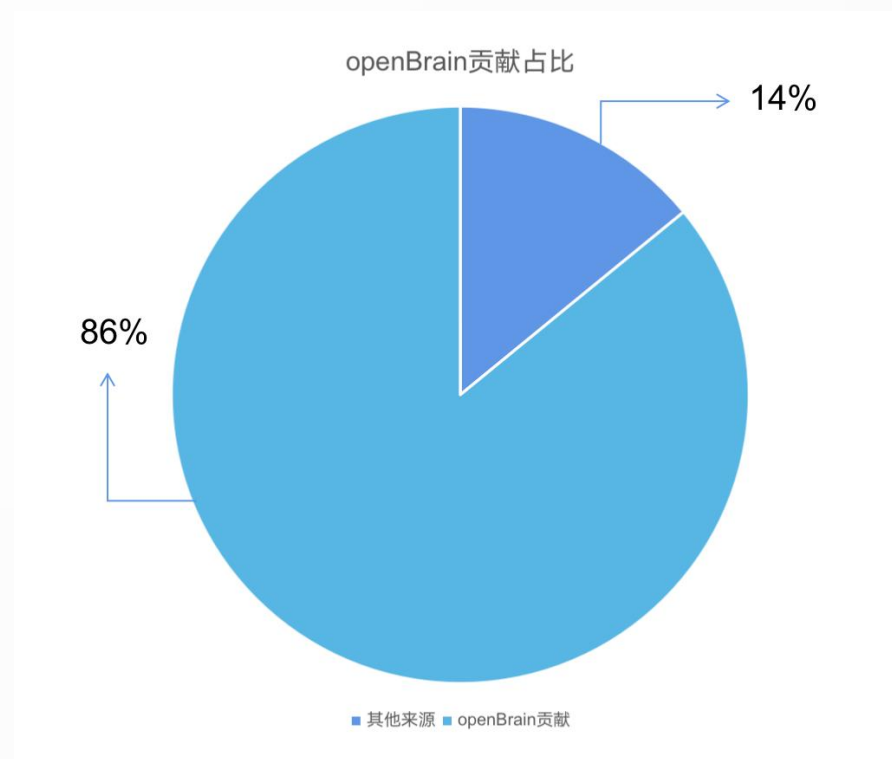
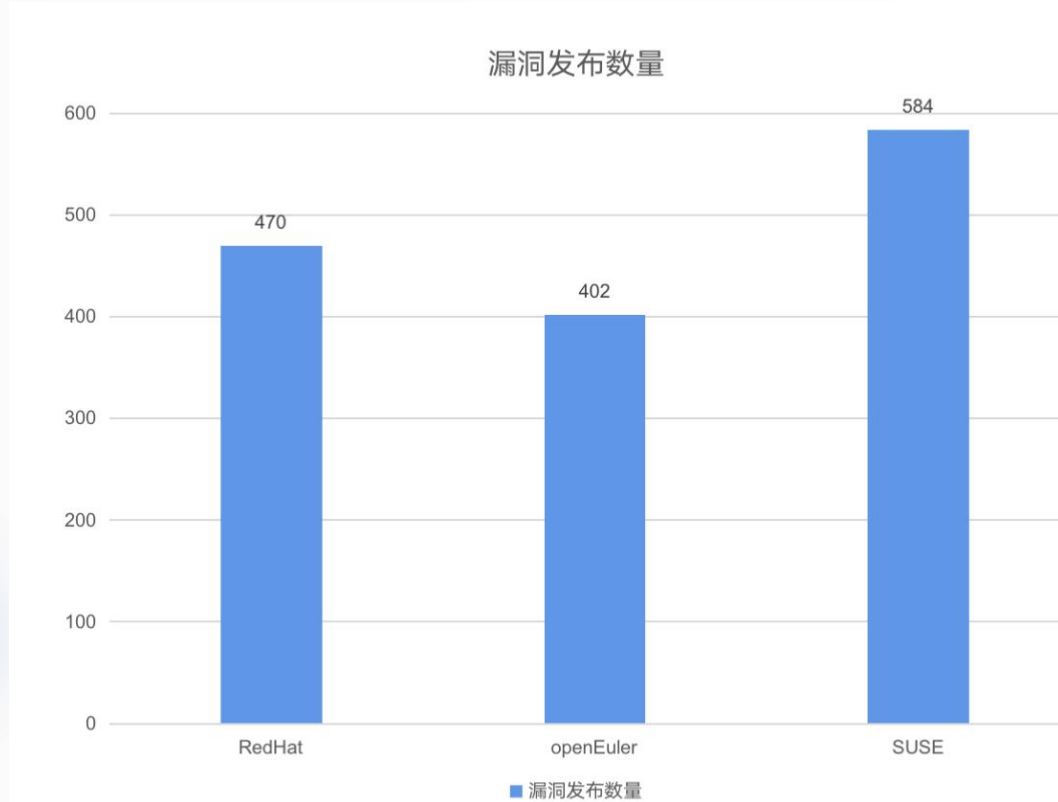
- 2022年9月和10月，openBrain达到最高准确率。

46天

时效性

- 2022年里，openBrain最早比NVD提前46天完成漏洞上报。

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）。





技术概述



技术进展



应用扩展

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。

探索

基金会

关于OpenAtom

开源大赛

搜索...

注册

登录

概览

精选

成员组织

代码库

Issues

变更请求

12 代码库

7 成员

北京

https://www.openatom.org/

sponsorship@openatom.org

关注

成员组织

ubml

26 代码库

5 成员

vearch

6 代码库

2 成员

hapjs

3 代码库

1 成员

Tongsuo

2 代码库

3 成员

linglong

6 代码库

1 成员

开源大师兄

12 代码库

2 成员

查看全部

成员

查看7个成员

精选

xupercore

公开

开放原子超级链内核XuperCore，定位为广域适用、高可扩展、超高性能、高度易用，并且完全自由开放的区块...

☆ 18

👤 2

taro

公开

开放式跨端跨框架解决方案，支持使用 React/Vue/Nerv 等框架来开发微信/京东/百度/支付宝/字节跳动/ QQ ...

☆ 6

👤 0

TencentOS-Tiny

公开

TencentOS Tiny（待更名）是开放原子开源基金会孵化的，面向物联网领域开发的实时操作系统，具有低功耗...

☆ 11

👤 0

OpenSource-Knowledge

公开

收集、整理、记录和开源相关的基础理论知识

☆ 19

👤 2

代码库

搜索代码库...

重置

默认排序

OPENATOM

开放原子开源基金会是致力于推动全球开源事业发展的非营利机构，于2020年6月在北京成立，由阿里巴巴、百度、华为、浪潮、360、腾讯、招商银行等多家龙头企业联合发起。

https://www.openatom.org/

sponsorship@openatom.org

9.1K 仓库

2.5K PR

1.2K Star

41.5K Fork

漏洞风险

后门/设备

维护性风险

合规风险

组件名称

影响版本

上游项目地址

组件支持情况

威胁类型

首次最新检测时间

jettison

120

notebook

6.4.9

https://github.com/viaze

官方已于2020-06-09停止更新

停服风险、断供风险

2023-03-22 14:31:48

keyutils

30

node-mkdirp

0.5.1.2

https://github.com/sub

官方已于2018-12-10停止更新

停服风险

2023-03-22 14:31:48

gitables

13

runc

10

CodeTest

xxxx

https://github.com/cod

官方已于2023-03-21停止更新

断供风险

2023-03-23 00:00:00

ca-certificates

8

shiro-redis

xxxx

https://gitee.com/BYS

官方已于2022-01-30停止更新

断供风险

2023-03-22 14:31:48

elasticsearch

6

风险管理 / 漏洞详情

Jettison不受控制的递归漏洞

不受控制的递归

Apache Struts2

漏洞详情公开

CVE-2023-1436

3

90+

受影响产品/组件

受影响版本

12

1.2K

安全版本

相似漏洞

发布时间

Poc

官方补丁

2023-03-22

有

有

PoC下载地址1: https://xxx/xxx

PoC下载地址2: https://xxx/xxx

影响范围

Apache Struts2

by Apache license: GPL-2.0

6个版本

12天前发布

Spring Boot

by Pivotal Software

12个版本

1个月前发布

Hadoop Hive

by Apache license: GPL-3.0

3个版本

1个月前发布

软件包

影响版本

CPE

apache-log4j1

2.X

cpe:/o:xxxx:xxxx_xxx_2021

apache-log4j2

<3.X

cpe:/o:xxxx:xxxx_xxx_2021-r1

apache-log4j3

>4.X

cpe:/o:debian:debian_linux:2.1.8.8:p3:1.1

修复建议

USN-4151-1: Python vulnerabilities

Ubuntu 19.04

升级 python2.7 至 2.7.16-2ubuntu0.2 版本

升级 python2.7-minimal 至 2.7.16-2ubuntu0.2 版本

升级 python3.7 至 3.7.3-2ubuntu0.2 版本

查看

添加

安全公告

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

9.3 High

CVSS2

10 High

CVSS3

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Changed

Confidentiality Impact

High

Integrity Impact

High

Availability Impact

High

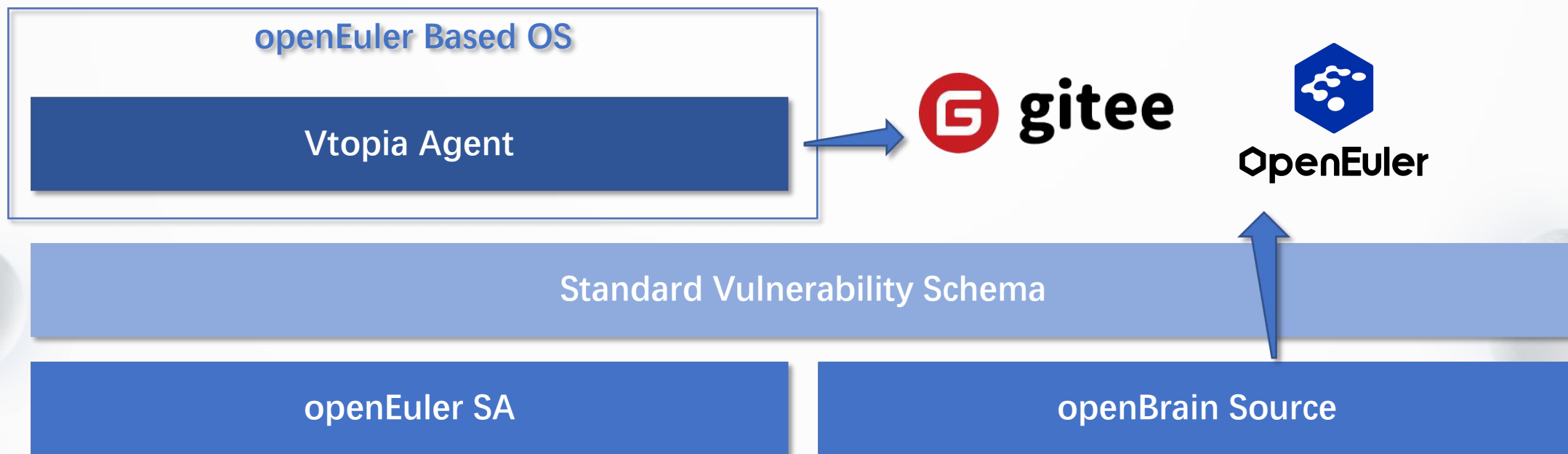


oepkgs 全称为开放软件包服务（Open External Packages Service），是一个为openEuler以及其他Linux发行版提供软件包服务的第三方社区。openBrain能力引入oepkgs，实现oepkgs托管软件包的常态化漏洞感知能力，提供漏洞感知、动态优先级评估、关键漏洞预警、关键知识推送等服务。

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。



THANKS