



开源软件安全 实践与思考

黄永刚

奇安信代码安全实验室 主任

- 奇安信旗下专注于软件源代码安全分析技术、二进制漏洞挖掘技术研究的实验室。国家发改委“大数据协同安全技术国家工程实验室-代码安全实验室”的承担单位，负责国家工程实验室在软件安全开发、软件漏洞分析等方面的研究工作规划和组织实施
- 自主研发了国内第一个源代码安全分析系统，可检测1300多种源代码安全缺陷，应用于超过150家国内大型机构
- 通过技术研究和自研产品，帮助微软、Cisco、Adobe、苹果、Oracle、Linux内核组织、SAP、Facebook、IBM、Apache基金会、阿里云、华为、Netgear、Dlink等大型厂商或开源组织修复了300多个软件安全缺陷和漏洞
- 在Pwn2Own 2017世界黑客大赛上，奇安信代码安全实验室研究人员成功攻破Adobe、微软等高难度项目，并获得Master of Pwn破解大师世界冠军称号

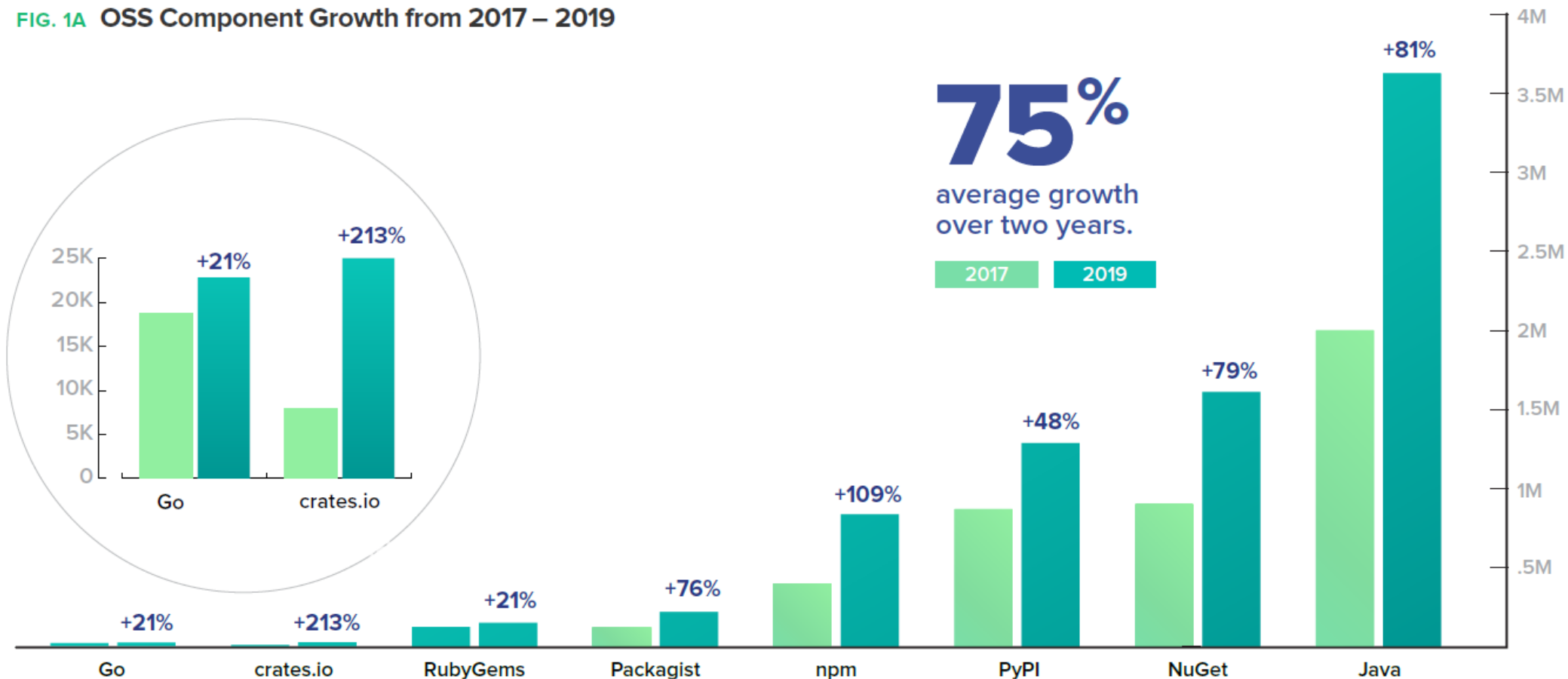
目录

- 1、开源软件安全现状
- 2、开源软件安全实践
- 3、思考与展望

目录

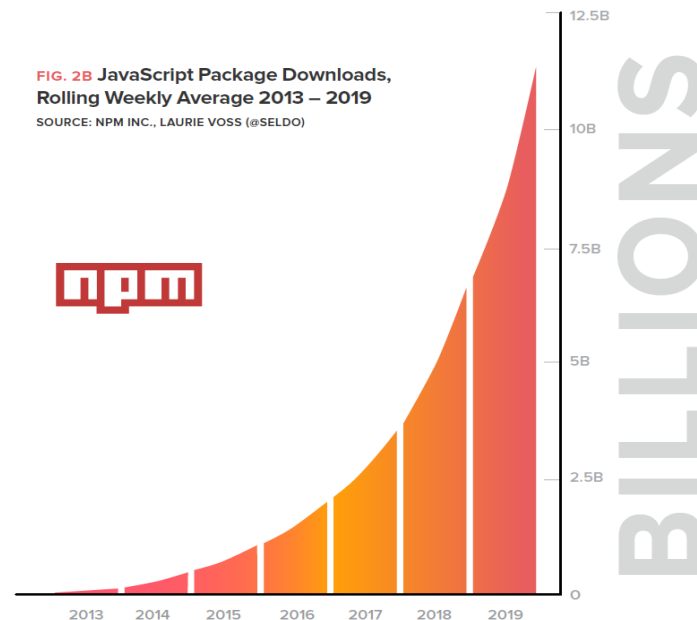
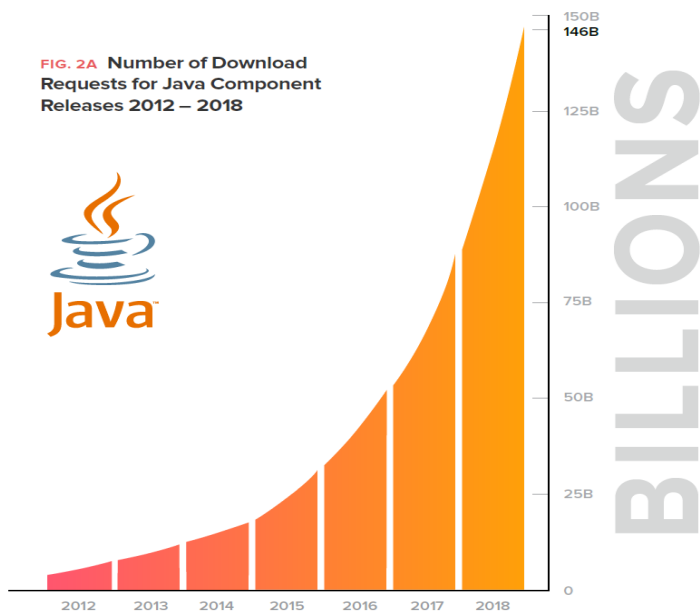
- 1、开源软件安全现状
- 2、开源软件安全实践
- 3、思考与展望

FIG. 1A OSS Component Growth from 2017 – 2019



注：数据来源于SONATYPE 2019 STATE OF THE SOFTWARE SUPPLY CHAIN REPORT

- Gartner: 99%的组织在其IT系统中使用了开源软件
- Gartner: 现代软件大多数是被“组装”出来的，不是被“开发”出来的
- Forrester: 软件开发中，80-90%的代码来自于开源软件



注：数据来源于SONATYPE 2019 STATE OF THE SOFTWARE SUPPLY CHAIN REPORT

美国征信巨头 Equifax 日前确认，黑客利用其系统中未修复的 Apache Struts 漏洞（CVE-2017-5638，3 月 6 日曝光）发起攻击，导致了最近影响恶劣的大规模数据泄漏事件。Equifax 是美国三大老牌征信机构之一，拥有大量美国公民敏感数据，收益一直在 10 亿级别。其原本提供免费信用监控和身份窃取保护服务，还声称可以安全地冻结对敏感信息的访问。此次大规模数据泄露对其而言无疑是一场灾难。



Spring 框架及组件存在多个安全漏洞

来源: 阿里云安全

发布日期: 2018-07-30



威胁快报 | 首个Spark REST API未授权漏洞利用分析

阿里云安全 | 2018-07-30 共134718人围观，发现1个不明物体 | WEB安全 | 漏洞

2018年7月7日，阿里云安全首次捕获Spark REST API的未授权RCE漏洞进行攻击的真实样本。7月9号起，阿里云平台已能默认防御此漏洞的大规模利用。

这是首次在真实攻击中发现使用“暗网”来传播恶意后门的样本，预计未来这一趋势会逐步扩大。目前全网约5000台 Spark服务器受此漏洞影响。阿里云安全监控到该类型的攻击还处于小范围尝试阶段，需要谨防后续的规模性爆发。建议受影响客户参考章节三的修复建议进行修复。

一、漏洞详情说明

Apache Spark 是为大规模数据处理而设计的快速通用的计算引擎。是UC Berkeley AMP lab(加州大学伯克利分校的AMP实验

你的数据安全么? Hadoop再曝安全漏洞 黑客利用Hadoop Yarn资源管理系统未授权访问漏洞进行攻击

2018年05月08日 10:59:59 | 阅读量: 751

CSDN 版权声明: 本文为博主原创文章, 未经博主允许不得转载。https://www.csdn.net/article/720845-1

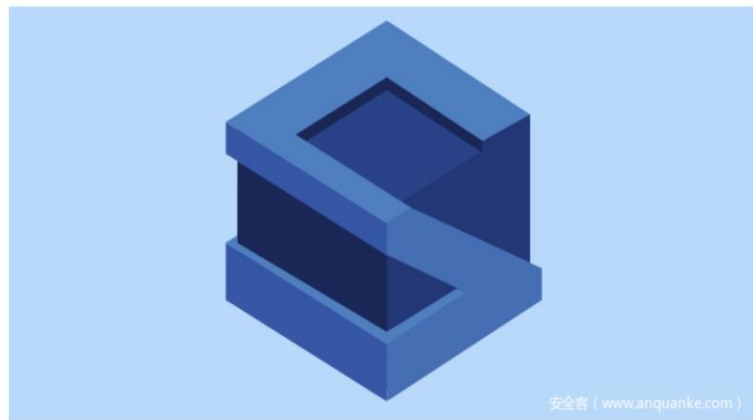
摘要: 4月30日, 阿里云发现, 俄罗斯黑客利用Hadoop Yarn资源管理系统通过著名的 MapReduce 算法进行分布式处理, Yarn是Hadoop集群

漏洞预警 | Apache Struts 2漏洞 (CVE-2018-11776/S2-057)

阅读量 720845 | 评论 16

发布时间: 2018-08-22 17:01:24

分享到: 微博 微信 知乎 豆瓣 贴吧 论坛



安全客 (www.anquanke.com)

概述

定义XML配置时如果namespace值未设置且上层动作配置 (Action Configuration) 中未设置或用通配符namespace时可能会导致远程代码执行。

url标签未设置value和action值且上层动作未设置或用通配符namespace时可能会导致远程代码执行。

目录

1、开源软件安全现状

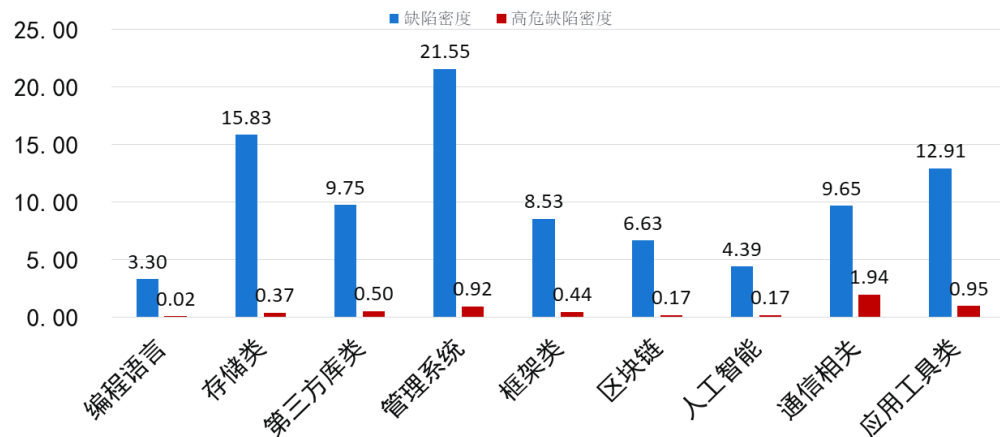
2、开源软件安全实践

- 奇安信开源项目检测计划
- 奇安信固件安全检测计划
- 企业开源软件安全治理实践

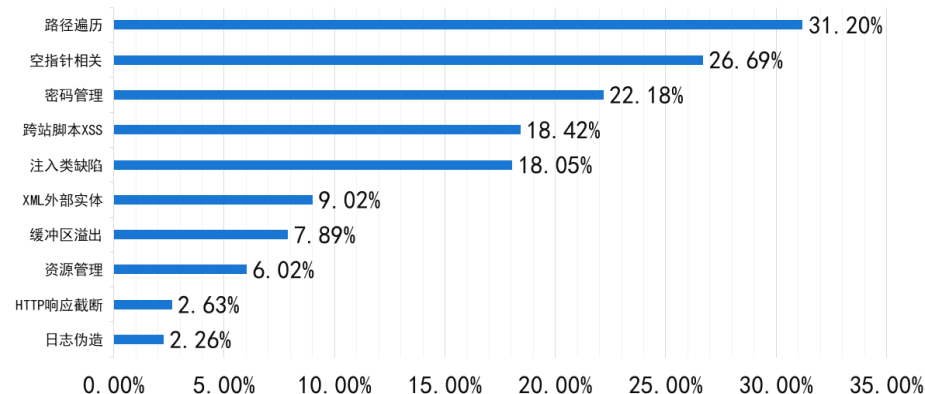
3、思考与展望

- 美国：自2006年开始，美国国土安全部资助开展了“开源项目检测计划”，目前已检测7000多款开源软件
- 2015年初，奇安信代码安全实验室基于自研产品和漏洞研究能力，发起了国内最大的“开源项目检测计划”，该计划目前已检测3000余款开源项目，积累了大量的开源软件安全缺陷基础数据
- 2018开源项目检测计划数据：
 - 缺陷密度：14.22/KLOC，高危缺陷密度：0.72/KLOC
 - 十类重要缺陷检出率：61.7%

各功能类开源项目的缺陷密度统计情况

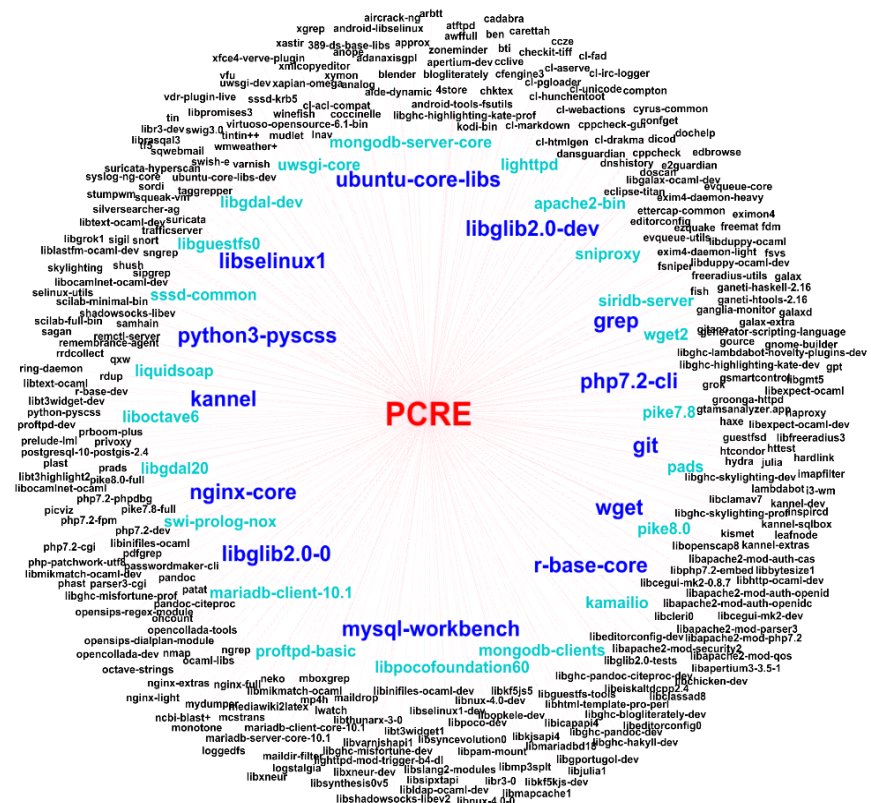


10类重要缺陷的总体检出率排名



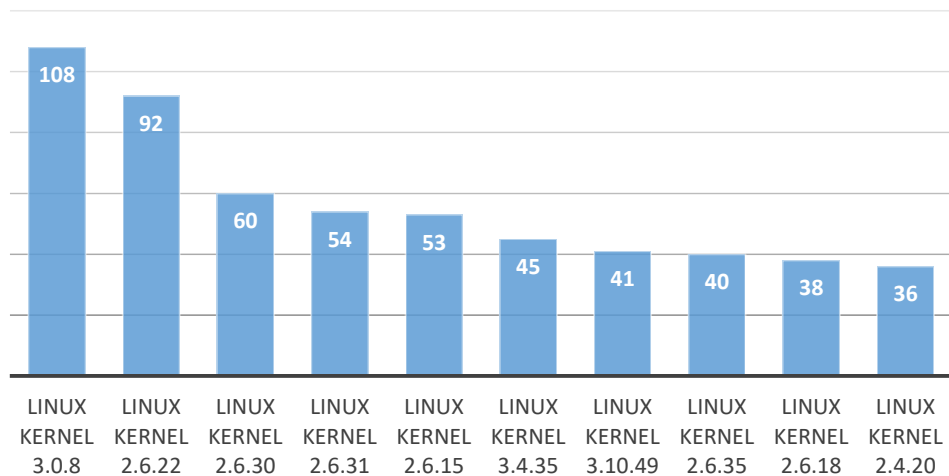
- 开源软件之间依赖关系错综复杂，漏洞的隐蔽传染和放大效果显著，给漏洞发现、漏洞消控带来了很大的挑战
- 某个开源软件出现漏洞，你可能会“躺枪”

开源组件	功能介绍	历史漏洞	直接关联 组件数量	间接关联 组件数量
Jsoup	一款Java 的HTML解析器，可直接解析某个URL地址、HTML文本内容。在Web开发中应用广泛。	CVE-2015-6748等	1829	16607
Log4j	Apache的一个开源项目，用于日志控制、生成等的管理和操作。广泛应用于Apache的Java日志管理中。	CVE-2017-5645等	4143	46006
Commons Collections	一款对JDK已有的数据结构进行补充和扩展的集合库，广泛应用于Java程序开发中。	CVE-2015-6420等	4922	81374
MySQL Connector/ J	MySQL的官方JDBC驱动程序，广泛用于MySQL数据存储中。	CVE-2019-2692等	3607	36049

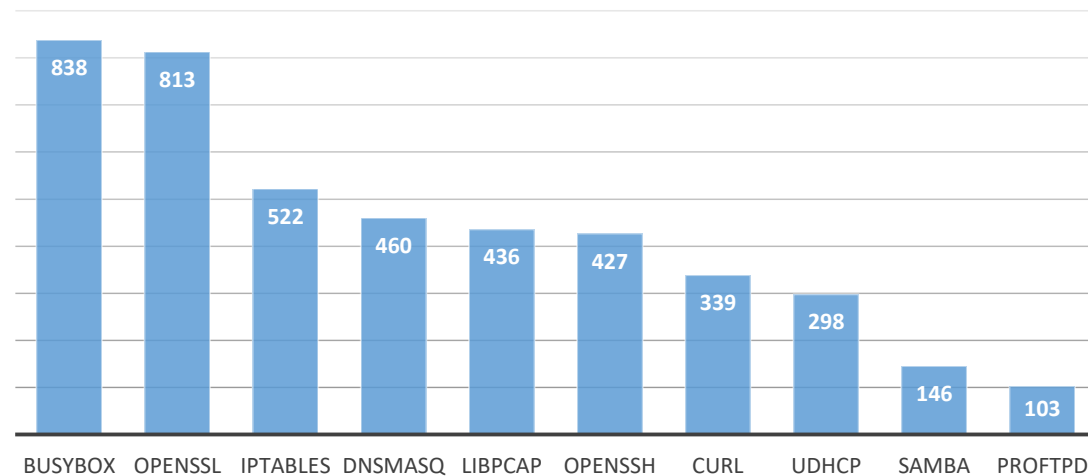


- 奇安信代码安全实验室2019年初发起的，针对联网设备固件的安全检测计划，其中一项重要检测内容是针对固件中引用的开源软件的检测和漏洞分析
- 2019年上半年，选取了**13个厂商935个设备的最新版固件**进行分析（以无线路由器、智能摄像头等可公开获得固件的设备为主）
 - 89.6%**基于Linux开源生态
 - 使用的开源软件版本五花八门，Linux内核版本50个，版本最多的开源软件是Openssl，存在77个版本

Linux Kernel版本TOP 10

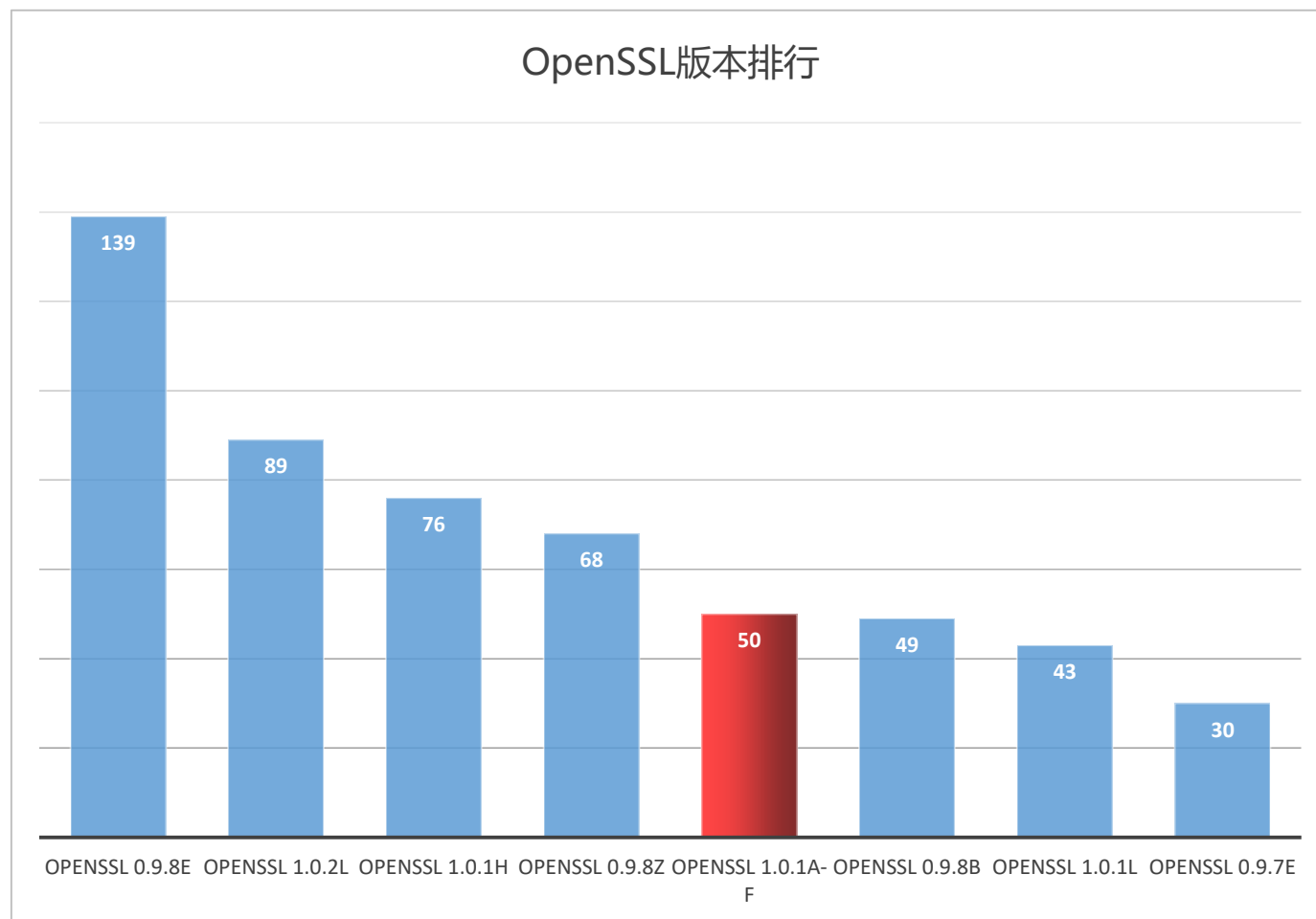


开源软件使用TOP 10



- 86.4%的固件存在至少一个老旧开源软件漏洞
- 漏洞最多的固件存在74个老旧开源软件漏洞

开源软件	CVE漏洞数	漏洞影响固件数	固件总数
OpenSSL	200	745	813
OpenSSH	92	291	427
curl	63	235	339
Dnsmasq	13	294	460
BusyBox	12	808	838



3个大型开发团队，67个软开项目

具体实践内容：

- 1、开源软件识别与关联分析——用了哪些？
- 2、开源软件漏洞分析——有没有漏洞？
- 3、开源软件漏洞修复——怎么修复？

- **100%**使用开源软件
 - 67个项目均使用了开源软件，无一例外
 - 使用的开源软件数量，最少的2个，最多的**567**个，平均**157**个
- 使用的开源软件的数量超出自己的想象
 - 层层嵌套的组件依赖
 - 当前的开发生态，包管理器替程序员自动做了很多他并没有意识到的决定
 - 开源软件资产的梳理需要系统化的方法，自动化的工具

项目	我以为我用了这么多	实际上我用了这么多
项目1	78	252
项目2	78	237
项目3	24	113
项目4	30	178
项目5	30	106
项目6	22	145



- 88%的项目因使用开源软件引入了安全漏洞
 - 59个项目存在开源软件漏洞，占比88%
 - 53个项目存在高危以上漏洞，占比79%
 - 28个项目存在超危漏洞，占比42%
- 平均每个项目存在44个开源软件漏洞
 - 漏洞最多的项目存在149个开源软件漏洞
- 开源组件漏洞情报的收集和漏洞精确匹配是一个很大的挑战
 - 漏洞情报源分散
 - 组件间的依赖关联，给漏洞情报的建立带来很大挑战

- Kubernetes Kubelet本地提权漏洞
 - NVD的描述
 - 没有?
 - Github上的详细信息
 - In kubelet v1.13.6 and v1.14.2, containers for pods that do not specify an explicit runAsUser attempt to run as uid 0 (root) on container restart, or if the image was previously pulled to the node. If the pod specified `mustRunAsNonRoot: true`, the kubelet will refuse to start the container as root. If the pod did not specify `mustRunAsNonRoot: true`, the kubelet will run the container as uid 0.
 - <https://github.com/kubernetes/kubernetes/issues/78308>

- Apache Log4j安全漏洞
 - NVD的描述
 - In Apache Log4j 2.x before 2.8.2, when using the TCP socket server or UDP socket server to receive serialized log events from another application, a specially crafted binary payload can be sent that, when deserialized, can execute arbitrary code.
 - 实际上，Apache Ant的1.9.9/1.10.1以及之前的版本，都会受到这个漏洞的影响，因为Apache Ant Log4jListener中使用了Apache Log4j库的受影响版本
 - 而我们从漏洞库的相关信息，找不到任何关于apache ant的蛛丝马迹

- Pippo安全漏洞?
 - NVD的描述
 - parseObject in Fastjson before 1.2.25, as used in FastjsonEngine in Pippo 1.11.0 and other products, allows remote attackers to execute arbitrary code via a crafted JSON request, as demonstrated by a crafted rmi:// URI in the dataSourceName field of HTTP POST data to the Pippo /json URI, which is mishandled in AjaxApplication.java.
 - 实际上根源是Fastjson的反序列化漏洞
 - https://github.com/alibaba/fastjson/wiki/security_update_20170315
 - 我们从漏洞库的参考信息中可以得到一些线索，但是其NVD给出的受影响产品版本中，还是不包含Fastjson的版本
 - 而Fastjson这个反序列化的洞，一直在持续进行修复
 - https://github.com/alibaba/fastjson/wiki/update_faq_20190722
 - <https://github.com/alibaba/fastjson/releases>

- 谨慎，谨慎，再谨慎
- 不能简单通过升级新版本或打补丁来修补漏洞
- 修复漏洞前，需全面评估对业务的影响
 - 业务系统复杂，不同部件协同工作，需考虑兼容性
 - Spark, Cassandra, Spark-Cassandra-Connector
 - 开源软件间的依赖关联，牵一发动全身
 - A被B, C, D依赖
- 需求：精准修复漏洞，不更改功能特性
 - 需要专业的漏洞研究队伍

- 2019.04.10 JQuery 发布版本3.4.0，更新内容包含对CVE-2019-11358的修复，但是没有针对1.x、2.x版本的补丁
- 客户软开项目中使用1.x，2.x 版本，无法升级到最新版本，故需要漏洞分析专业人员提供修复解决方案
 - 分析漏洞原理，完成漏洞详情分析报告
 - 详细分析官方修复代码，基于此制作多版本修复patch
 - 对patch进行兼容性验证，分析验证patch后对原有系统产生的影响
 - 制作POC，以验证patch的有效性
 - Patch+验证生效

目录

1、开源软件安全现状

2、开源软件安全实践


3、思考与展望

- 开源软件的使用形成了非常宽广、复杂、隐蔽的攻击面
 - 代码的复用→漏洞的复用，类似病毒的传播效应
 - 国内大型金融机构开源软件使用统计
 - 直接使用的开源软件1500+，再加上依赖的开源软件？漏洞都修复了吗？
 - 版本繁多，最多的一个开源软件，有14个版本同时在使用，考虑了运维成本吗，考虑了安全问题吗？
- 开源软件安全治理工作应尽量左移
 - 从软件开发阶段就建立开源软件使用的统一策略
 - 用什么、用什么版本、确认来源
 - 建立安全准入机制，引入开源软件前先评估安全风险
 - 持续检测，持续跟踪漏洞情报和响应
 - 外包开发的软件应在立项之初提出要求，并在验收时进行检查
- 开源软件安全治理是软件安全开发的首要事
 - 软件开发中，开源软件的不当使用是最大的安全风险
 - 开源软件治理对安全的促进作用成效显著，立竿见影

- 漏洞情报 ≠ CVE，开源软件的五种漏洞
 - Nday：已公开的漏洞，通常CVE收录
 - 0Day：未公开的漏洞
 - 0.5Day：半公开的漏洞，隐藏在代码提交日志、缺陷管理系统等
 - 关联漏洞：由组件依赖导致的漏洞
 - 克隆漏洞：代码Copy&Paste导致的漏洞
- 要描述Dev阶段的安全威胁，漏洞库需要全新升级
 - 多方数据来源，尤其是开源开发社区的信息来源
 - 漏洞情报数据的治理，建立漏洞-组件之间的全关联
 - CPE/CVE -> new SWID/VULID，自动化是目标，还要保持兼容

- SCA融入DevOps流程
 - Repo FW
 - SCA on demand
 - 安全状态跟踪
- 漏洞代码的精准定位，辅助修复
- 关注开源软件中的恶意代码
 - 例如，盗取SSH keys、API keys等敏感信息
 - 复杂的供应链攻击

- 对于企业
 - 使用开源软件可以降低成本，提高效率，有利于专注业务，是必然选择
 - 但是需要正确的、安全的使用开源软件
- 对于管理部门
 - 开源软件已经成为构筑网络空间的最基础的“砖头瓦块”，无处不在
 - 开源软件安全问题应该上升到基础设施安全的高度来对待，得到更多的、更广泛的重视



THANKS

2019 北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE