国家信息安全漏洞库
China National Vulnerability Database of Information Security

信息安全漏洞态势报告

（2015 年度）

中国信息安全测评中心

二〇一六年一月

（本页为空白页）

目　录

信息安全漏洞态势报告（2015 年度）

一、概述

随着网络和信息化建设的飞速发展，社交网络、移动互联网、大数据、云计算、物联网等新技术与新应用不断涌现，网络安全和信息安全问题已成为事关国家安全的重大问题，成为影响经济、政治、社会等诸多领域持续发展进步的关键因素。

受限于现有计算机系统结构、产业基础、工程方法、开发周期、安全意识、资金人力投入等诸多因素，信息技术产品及应用系统在设计、实现、部署、运行、维护等阶段不可避免地存在各种安全缺陷，从而直接或间接地导致各种信息安全事件的发生。信息安全漏洞主要指在信息技术、产品及系统在需求、设计、实现、配置、维护和使用等过程中，所产生的安全缺陷。这些缺陷被利用，就会造成对信息产品或系统的安全损害，从而影响正常服务运行，危害信息安全。

国外政府高度重视对漏洞资源的管控，通过建立完善的国家漏洞管理体系，将漏洞资源纳入国家管控机制。2006 年，美国政府在 ICAT Metabase（http://icat.nist.org）的基础上建立了美国国家漏洞库（National Vulnerability Database，NVD），由国土安全部（Department of Homeland Security，DHS）研究部署并提供建设资金，由美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）负责技术开发和运维管理。2015 年 5 月，美国商务部工业与安全局公布了“瓦森纳协定”的一份补充协定，把黑客技术放入全球武器贸易条约出口限制的范围内，限制零日漏洞及其相关产品流出美国。

中国政府高度重视网络和信息安全问题，重视对信息安全漏洞的管控。2007 年，中国信息安全测评中心负责建设运维国家级漏洞资源管理平台“国家信息安

全漏洞库”（China National Vulnerability Database of Information Security，CNNVD）。2009 年 10 月 18 日，国家信息安全漏洞库网站正式上线运行，对外提供漏洞分析、通报服务。经过多年发展建设，CNNVD 通过社会提交、协作共享、网络搜集以及技术检测等方式，已积累信息技术产品漏洞 8 万余条，信息系统相关漏洞 4 万余条，相关补丁和修复措施 2 万余条，初步形成了信息安全漏洞的资源汇聚和处置管理能力。

鉴于信息安全漏洞重要性逐渐增强及其威胁程度日益提升，CNNVD 基于已收录的信息安全漏洞情况，对 2015 年度信息安全漏洞数据进行统计分析，总结漏洞分布特点，形成了 2015 年度信息安全漏洞态势报告。

本报告主要包括六部分内容。第一部分为概述。第二部分主要针对 CNNVD 收录漏洞情况，从数量增长、类型分布、危害等级、影响产品等方面进行了统计分析。第三部分列举 2015 年全年漏洞数量统计排名靠前的重要厂商，对其主要产品的漏洞分布情况和发展趋势进行了对比分析。第四部分对 2015 年漏洞问题较为突出的开源软件进行梳理和分析，筛选出危害级别较高、影响范围较广的十大漏洞。第五部分针对国外漏洞管理法律法规、漏洞相关标准规范发展、漏洞交易市场化及国内安全响应机构情况进行了分析总结。第六部分为总结和对未来发展的展望。

二、2015 年信息安全漏洞基本情况

根据 CNNVD 统计，截至 2015 年 12 月 31 日，CNNVD 收录漏洞总量已达 80300 个，其中 2015 年新增漏洞 7754 个，与 2014 年漏洞新增的 8623 个相比有所下降，降幅为 10.08%。从漏洞类型来看，2015 年缓冲区溢出类的漏洞占比最大，达到 14.03%。从危害级别来看，2015 年新增危急漏洞 608 个、高危漏洞 1782 个、中危漏洞 4588 个、低危漏洞 776 个，其中 6659 个漏洞已发布修复补丁，整体修复率为 85.88%，四种危害级别漏洞对应修复率分别为 91.28%、92.48%、82.52%以及 86.34%。

2.1 漏洞数量年度统计分析

信息安全漏洞主要分为硬件漏洞和软件漏洞，其中软件漏洞又分为操作系统漏洞和应用软件漏洞。如图 1 所示，2015 年新增漏洞绝大多数为应用软件漏洞，达 5142 个，其次为操作系统漏洞，共 1788 个，而硬件设备漏洞数量仅为 65 个，由此可见应用软件漏洞仍是漏洞挖掘和分析的热点。

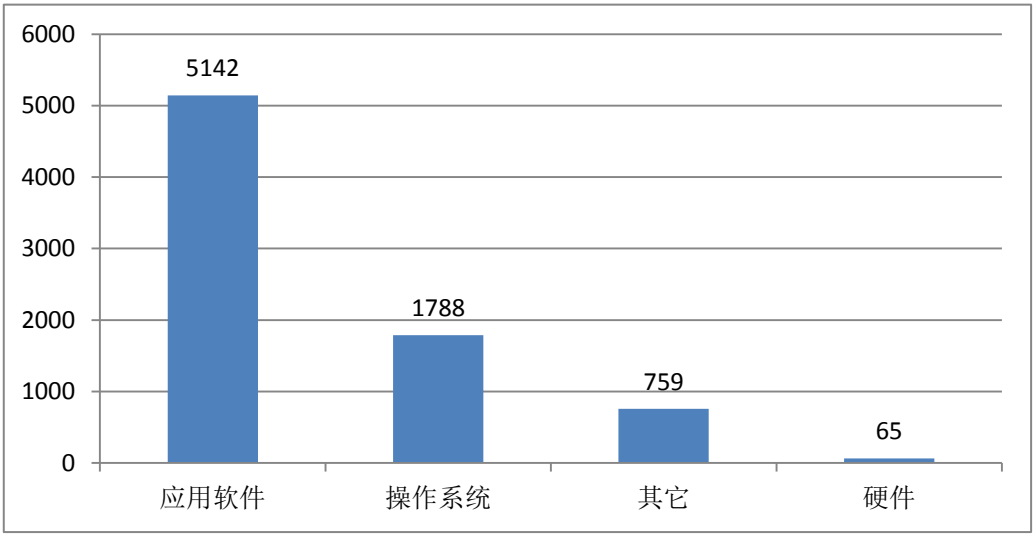

图 1　2015 年新增漏洞分布

如图 2 所示，自 2010 年来以来，新增漏洞数量呈现整体增加的趋势，从 2010 年的 4636 个，至 2015 年 7754 个，年均增加漏洞 6781 个，自 2012 年起，均维持在每年 7000 个以上，有 3 个年度漏洞数增幅量达到 20%。其中 2014 年的新增漏洞数量有较大增幅，这是因为 2014 年 9 月至 10 月，“Google Play”应用商店上近 1400 款 Android 应用程序被发现存在漏洞。这些漏洞是由于 Android 应用程序开发人员在编码时未能正确实现对服务器端证书认证的功能而导致的，该系列漏洞由卡内基梅隆大学计算机应急响应小组发现并发布。

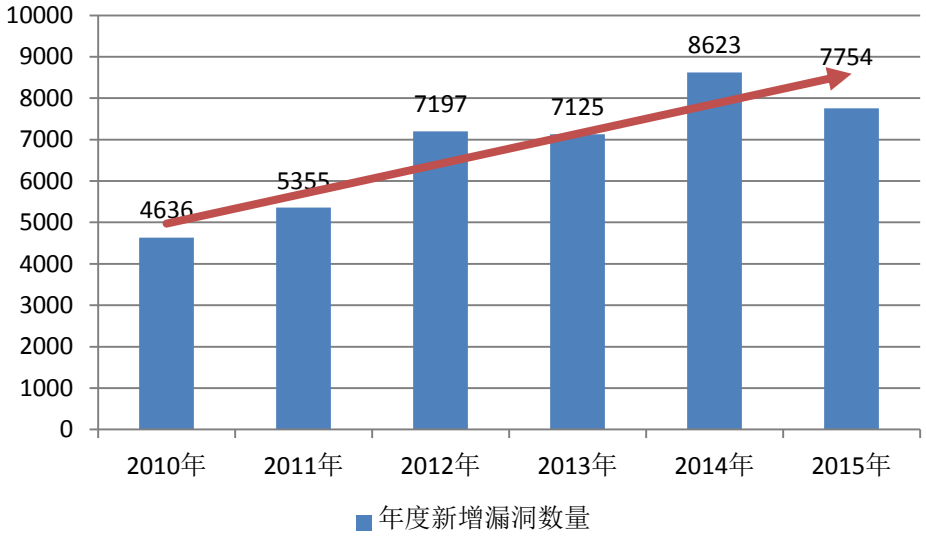

图 2　2010 年至 2015 年漏洞新增数量统计

2.2 漏洞类型分布统计分析

2015 年新增漏洞中，缓冲区溢出类漏洞数量最多，达 1088 个，占比高达 14.03%，与 2014 年该类型漏洞数量 787 个相比，增加了 38.25%。缓冲区溢出漏洞是出现非常频繁、且可能会带来严重后果的漏洞，利用缓冲区溢出漏洞，可以进行摧毁堆栈、上传木马、执行任意代码等多种形式的攻击，漏洞数量多、危害级别高，如何防范缓冲区溢出漏洞成为漏洞分析技术研究的热点问题。漏洞类型统计如表 1 所示。

表 1　2015 年漏洞类型统计表

序号	漏洞类型	漏洞数量	所占比例
1	缓冲区溢出	1088	14.03%
2	跨站脚本	817	10.54%
3	权限许可和访问控制	812	10.47%
4	信息泄露	712	9.18%
5	输入验证	531	6.85%
6	资源管理错误	395	5.09%
7	代码注入	271	3.49%
8	SQL 注入	268	3.46%
9	跨站请求伪造	267	3.44%
10	路径遍历	163	2.10%
11	数字错误	151	1.95%
12	加密问题	104	1.34%
13	信任管理	68	0.88%
14	授权问题	52	0.67%
15	操作系统命令注入	51	0.66%
16	竞争条件	51	0.66%
17	后置链接	23	0.30%

如图 3 所示，除漏洞数量最多的缓冲区溢出和跨站脚本类型外，权限许可和访问控制类型的漏洞数量也呈现出上升趋势。访问控制技术是实现 Web 应用系统安全目标的一个重要技术措施，安全研究人员对于权限管理的重视程度逐步加深，权限许可与访问控制类漏洞数量也在持续增多。

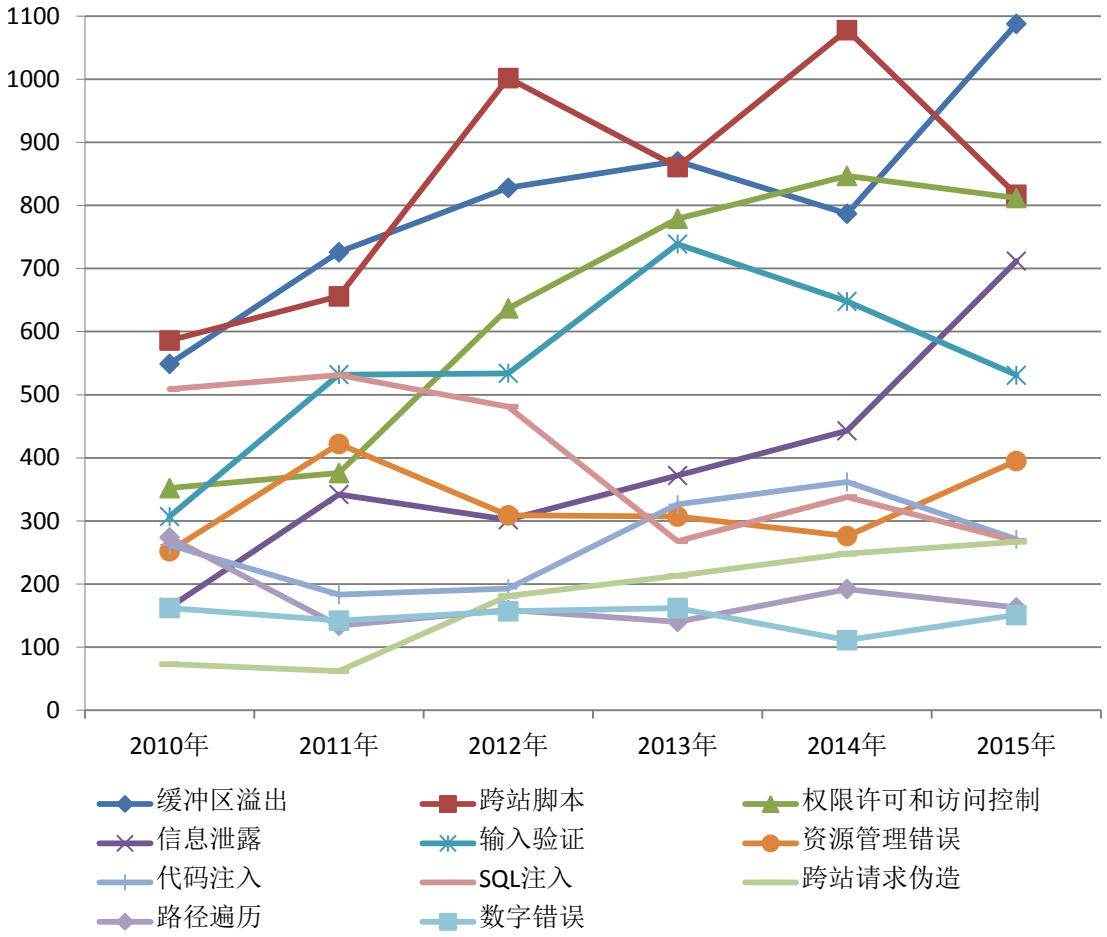

图 3　2010 年至 2015 年主要漏洞类型数量统计

2.3 漏洞危害等级分布统计分析

根据漏洞的影响范围、利用方式、攻击后果等情况，可将其分为四个危害等级，即危急、高危、中危和低危级别。2015 年漏洞危害等级分布如图 4 所示，近 6 年的漏洞危害等级分布如图 5 所示。根据 CNNVD 统计数据，四类漏洞中，以中危级别的漏洞数量居多，每年均占漏洞总量的一半以上。近年来，危害程度较高的危急和高危漏洞也开始呈现缓慢上升的趋势，2015 年数量超过 2000 个，占漏洞总量的 30.82%，比 2014 年增加近 300 个，占比增加 9.62%。漏洞被恶意攻击者利用，会对系统的正常运行造成破坏，进而影响业务工作，用户应当随时关注漏洞发布情况，及时采取打补丁、更新软件版本等消控措施，修复漏洞，

降低危害。同时，危害程度较高漏洞的占比逐渐上升也表明当前的信息安全形势仍然十分严峻，安全威胁不容轻视。

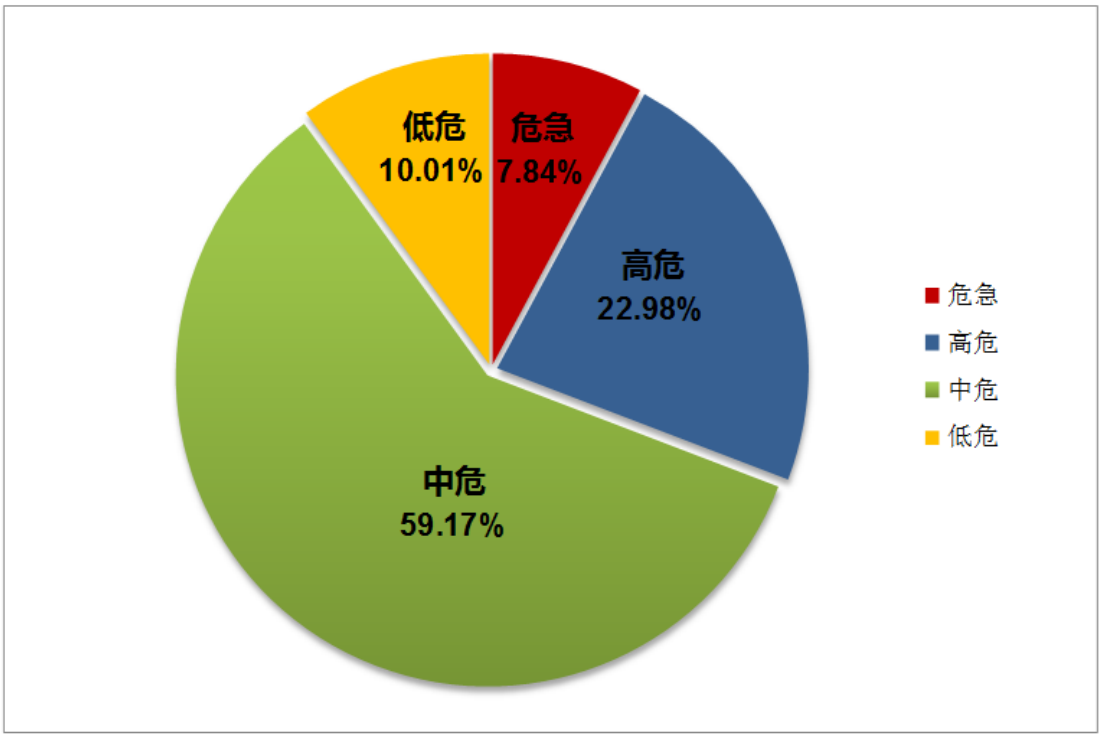

图 4　2015 年漏洞危害等级分布

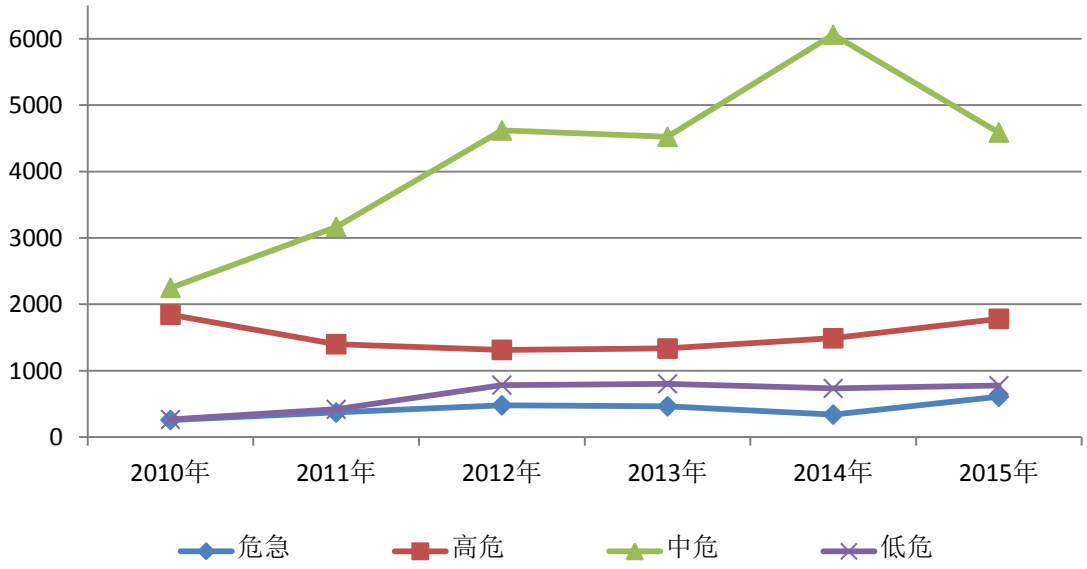

图 5　2010 年至 2015 年漏洞危害等级分布

2.4 漏洞影响产品分布统计分析

2.4.1 主流操作系统漏洞数据分析

操作系统（Operating System，OS）是管理和控制计算机硬件与软件资源的计算机程序，任何其他软件都必须在操作系统的支持下才能运行。根据应用领域，操作系统可以分为桌面操作系统、服务器操作系统、移动操作系统、主机操作系统和嵌入式操作系统等。根据 CNNVD 历年统计数据，操作系统漏洞多集中于前三类。2015 年 CNNVD 新增操作系统漏洞数量为 1788 个，其中 Mac OS X 和 Windows 系列桌面操作系统以及 iOS 移动操作系统漏洞数量最多，占操作系统漏洞总数的 41.28%。桌面操作系统方面，2015 年 Mac OS X 漏洞数量大幅度增长，达到 359 个，是 2014 年的 3 倍多，达到近年来的最高值；Windows 操作系统漏洞数量同样增长显著，达到 169 个，是 2014 年的 4 倍多。移动操作系统方面，iOS 系统漏洞达到 375 个，同比增长 212.50%；Android 系统漏洞达到 95 个，是 2014 年的 7 倍多。

下面主要针对近五年主流操作系统漏洞数量增长情况、主流操作系统和部分具体版本操作系统漏洞分布情况、以及针对主流操作系统漏洞研究的趋势进行统计和分析。其中，桌面操作系统主要包含 Windows 系列（Windows XP、Windows Vista、Windows 7、Windows 8、Windows 10 等）、Mac OS X 和 Linux（Ubuntu、Redhat、Fedora 等）；服务器操作系统主要包含 Windows Server 系列（Windows Sever 2003、Windows Sever 2008）、Linux、Unix（Solaris、AIX、HP-UX 等）和 Netware；移动操作系统主要包含 iOS、Android、Windows Phone、Symbian 等。

（1）主流操作系统漏洞年度趋势

2011 年至 2015 年操作系统漏洞数量如图 6 所示，2011 年以来操作系统漏洞整体呈上升趋势。2011 年和 2012 年操作系统漏洞为 580 个左右，2013 年跃升至 1057 个，是 2012 年的近 2 倍，2014 年趋势平稳，为 1033 个，2015 年又突增至 1788 个，达到历年来最大值。随着 Windows 10 的进一步推广，以及 Mac OS X 和 iOS 在企业用户市场占有率的不断提升，可以预测，2016 年操作系统漏洞仍将持续增长。

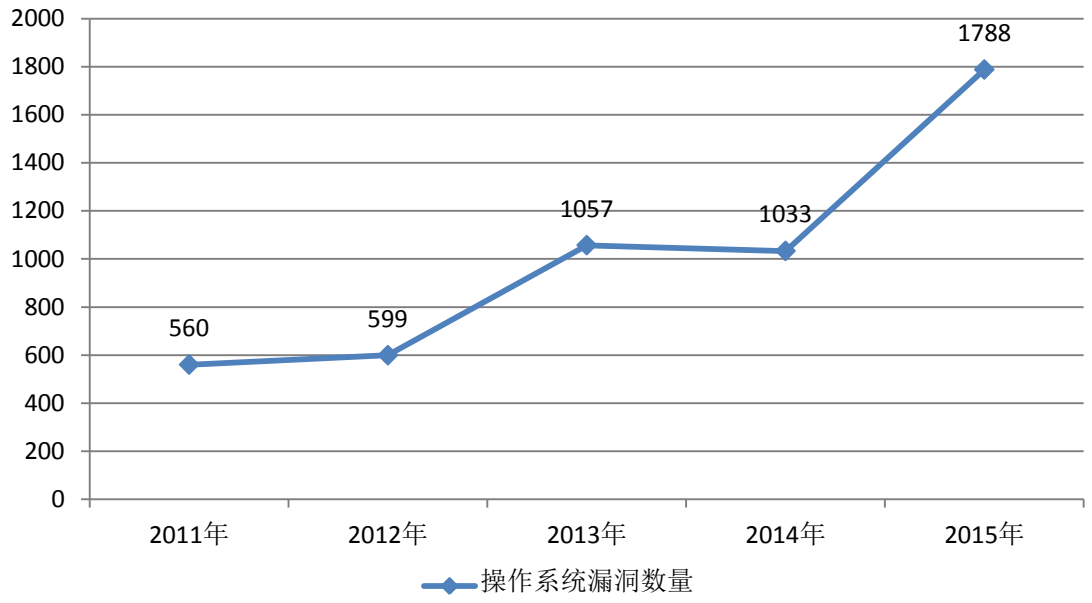

图 6　2011 年至 2015 年操作系统漏洞数量统计

（2）主流操作系统漏洞分布统计

桌面操作系统方面，截止至 2015 年 11 月，Windows 7、Windows 8.1、Windows 10、Mac OS X 是全球市场占有率最高的四大桌面操作系统。随着 Windows 10 的发布和推广，Windows 10 系统的市场占有率持续增长，对于 Windows 操作系统关注的提升，导致 2015 年 Windows 漏洞数量大幅度增长，达到 169 个，占主流操作系统漏洞总量的 9.45%，是 2014 年的 4 倍多；Mac OS

X 漏洞数量增长更为显著，达到 359 个，是 2014 年的 3 倍多，占主流操作系统漏洞总量的 20.08%，达到近年来的最高值。

移动操作系统方面，iOS 和 Android 系统占据了大部分市场份额，移动操作系统漏洞主要是 iOS 和 Android 系统的漏洞，而随着对移动操作系统进行漏洞分析和挖掘的人员逐渐增多，iOS 和 Android 系统的漏洞数量出现明显的增长，iOS 系统漏洞达到 375 个，是 2014 年的 3 倍多，占主流操作系统漏洞总量的 20.97%。

服务器操作系统方面主要由 Windows Server 系列和 Linux 系统主导，2015 年 Windows Server 系列操作系统网络主机方面的市场份额逐步提升，Windows Server 系列漏洞明显增多，是 2014 年的 4 倍多，Linux 系统漏洞数量明显减少，同比下降了 24.63%。

表 2　2015 年主流操作系统漏洞数量统计

序号	操作系统名称	类型	漏洞数量	所占比例
1	iOS	移动操作系统	375	20.97%
2	Mac OS X	桌面操作系统	359	20.08%
3	Windows Server 系列	服务器操作系统	171	9.56%
4	Windows 系列	桌面操作系统	169	9.45%
5	Linux	服务器操作系统	101	5.65%
6	Android	移动操作系统	95	5.31%

2011 至 2015 年主流操作系统漏洞数量年度分布如图 7 所示。由于 2011 年移动互联网尚未全面普及，安全人员的研究重点主要集中在桌面和服务器操作系统，2011 年 Linux 漏洞数量 147 个，排名第一，Windows 系列和 Windows Sever 系列漏洞数量紧随其后。而 2012 年 iOS 全球市场份额总大幅度上升至 65%，iOS 成为安全研究的热点，被发现的 iOS 漏洞数量也迅速增多，达到 112 个，超过 Linux 排名第一，这也表明安全研究人员开始关注移动平台。2013 年 Linux 漏洞

数量再次上升至第一名，达到 179 个，Windows 系列和 Windows Sever 系列也分别上升至 111 个和 108 个，是 2012 年的近 2 倍，而 iOS 漏洞数量有所减少，为 90 个，并在 2014 年持续减少。2014 年除 Mac OS X、iOS 和 Android 之外，所有操作系统漏洞数量均出现不同程度的减少。2015 年则是除了 Linux 之外，所有操作系统漏洞数量都呈现出明显上升趋势。

2011 年至 2014 年，Windows Sever 系列和 Linux 漏洞数量及波动情况基本相同，分别在 2012 和 2014 年出现两次比较明显的下降情况，在 2015 年 Windows Sever 系列漏洞数量增多，是 2014 年的 4 倍多，而 Linux 的漏洞数量持续下降，达到近年最低值 101 个。

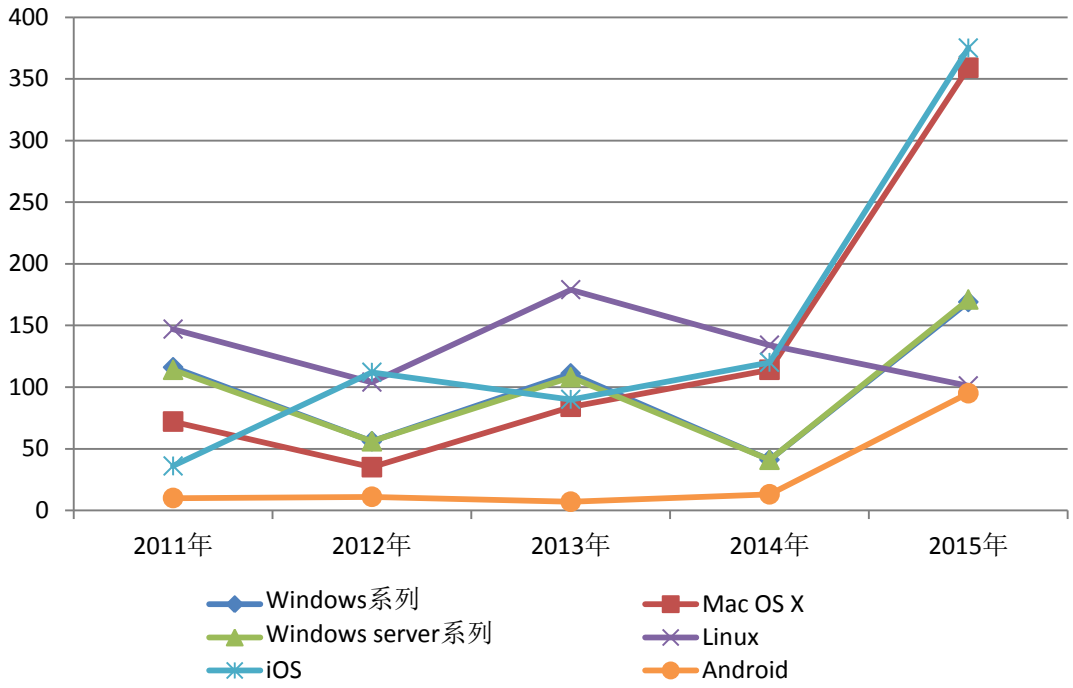

图 7　2011 年至 2015 年主流品牌操作系统漏洞数量年度分布

2011 至 2015 年桌面操作系统、移动操作系统和服务器操作系统漏洞数量如图 8 所示，桌面操作系统和移动操作系统整体呈上升趋势。2015 年之前，桌面操作系统和服务器操作系统漏洞数量和波动基本相近，平均数量约为 200 个，桌面操作系统漏洞数量在 2015 年增长较为明显，而服务器操作系统整体趋势较

为平缓，未出现较明显的波动，移动操作系统漏洞自 2013 年开始增长，2015 年出现大幅度的上升趋势，可见今年关注的重点主要是桌面操作系统和移动操作系统。

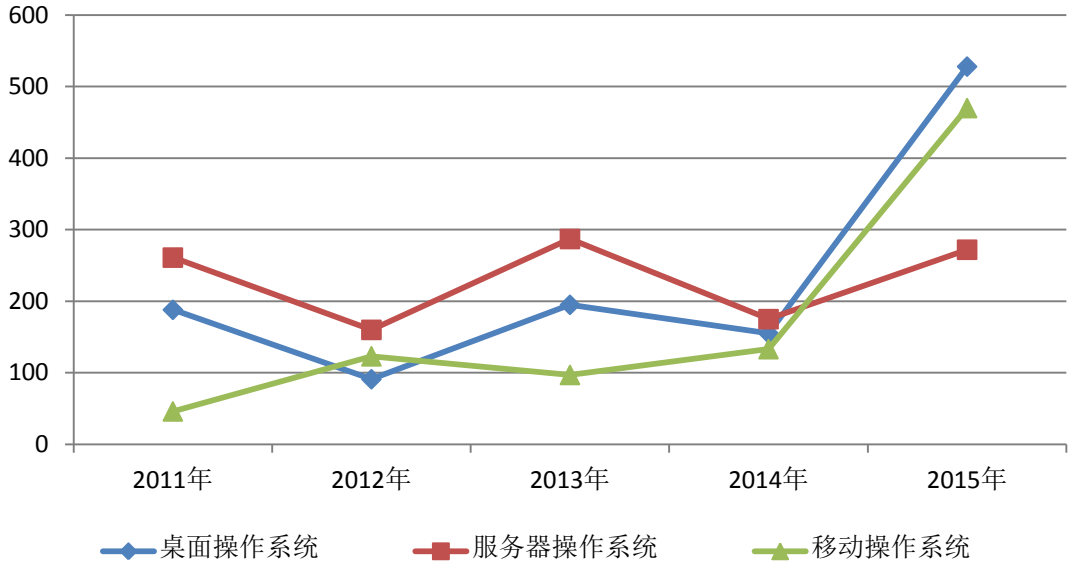

图 8　2011 年至 2015 年各类操作系统漏洞数量统计

2.4.2 主流浏览器漏洞数据分析

随着全球互联网普及率大幅度提升，网民规模进一步扩大，浏览器作为互联网基础应用发挥着越来越重要的作用，同时也越来越多的受到安全研究人员的关注。在近五年的世界知名黑客大赛 Pwn2Own 上，浏览器漏洞的挖掘和利用是重要环节。浏览器中集成了多种应用软件插件，这些插件在增强浏览器功能的同时，也因其自身的缺陷和漏洞带来了大量的安全风险。浏览器作为最易攻击和影响范围最广的对象之一，漏洞数量呈现缓慢上升的趋势，并在 2015 年达到最大增幅。同时，由于浏览器厂商的高度重视，主流浏览器漏洞的修复率都达到了 100%，很大程度上提高了用户上网的安全性。

目前全球浏览器市场的绝大部分市场份额被 Microsoft IE、Google Chrome、Mozilla Firefox、Apple Safari 和 Opera 这五款产品占据。2015 年浏览器产品的

漏洞总量为 779 个，是近五年最大值，同比增长 37.39%。其中 IE 浏览器虽然 2015 年漏洞数量同比减少，但是仍以 228 个的总量连续两年成为漏洞数量最多的浏览器。下面主要针对近五年主流浏览器漏洞数量增长情况和漏洞分布情况进行统计和分析。

（1）主流浏览器漏洞年度趋势

2011 年至 2015 年主流浏览器漏洞数量如图 9 所示，2011 年以来浏览器漏洞增长较为平缓，整体呈上升趋势，每年漏洞数量都在 500 个以上。其中，2011 年主流浏览器漏洞数量为 604 个，占当年漏洞总量的 11.28%，2012 年数量增长至 714 个，2013 年出现小幅度下降，仅为 508 个，是近五年最低值，2014 年开始，主流浏览器漏洞数量缓步上升，2015 年达到五年最大值 779 个。

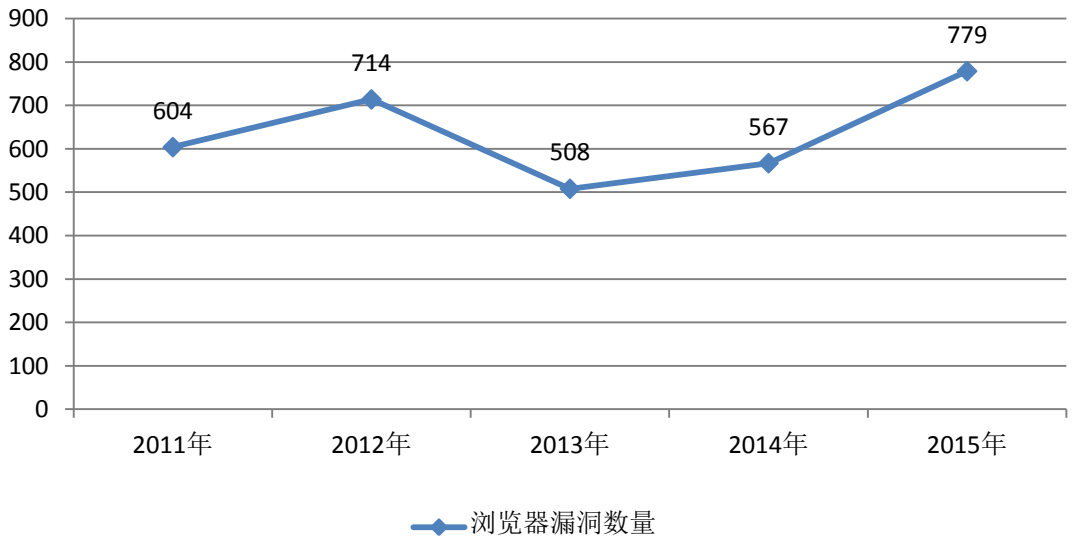

图 9　2011 年至 2015 年浏览器漏洞数量统计

（2）主流浏览器漏洞分布统计

2011 至 2015 年主流浏览器漏洞数量年度分布如图 10 所示，Microsoft Internet Explorer 和 Apple Safari 漏洞整体呈上升趋势，Mozilla Firefox 漏洞数

量有所波动，但都在 150 个上下，Google Chrome 和 Opera 漏洞数量呈下降趋势。

IE 漏洞在 2011 年仅 49 个，2012 年更是下降到 42 个，2013 年开始 IE 漏洞数量大幅度上升，达到 130 个，2014 年又是翻了一番，达到近五年最大值 243 个，首次成为当年漏洞数量最多的浏览器，2015 年 IE 漏洞数量有所下降，为 228 个，但仍占据浏览器漏洞数量的首位。

2011 年 Safari 漏洞数量为 50 个，2012 年上升至 88 个，2013 年出现大幅度下降，降至 17 个，2014 年有所回升，达到 71 个，2015 年 Safari 漏洞数量大幅增长，达到 135 个，比 2014 年翻了一番，达到近五年最大值。

Chrome 和 Opera 漏洞数量都呈现较为明显的下降趋势，Chrome 漏洞数量从 2011 年的 276 个，逐年下降，2014 年降至最低值 131 个，2015 年虽有所回升，但涨幅不大。Opera 在 2011 年漏洞数量为 65 个，与 Chrome 趋势相同，呈现逐年下降的趋势，2014 年数量最低为 2 个，2015 年仅为 5 个。

表 3　2015 年主流浏览器漏洞分布统计

序号	操作系统名称	漏洞数量	所占比例
1	Microsoft Internet Explorer	228	29.27%
2	Google Chrome	185	23.75%
3	Mozilla Firefox	184	23.62%
4	Apple Safari	135	17.33%
5	Opera Software Web Browser	5	0.64%

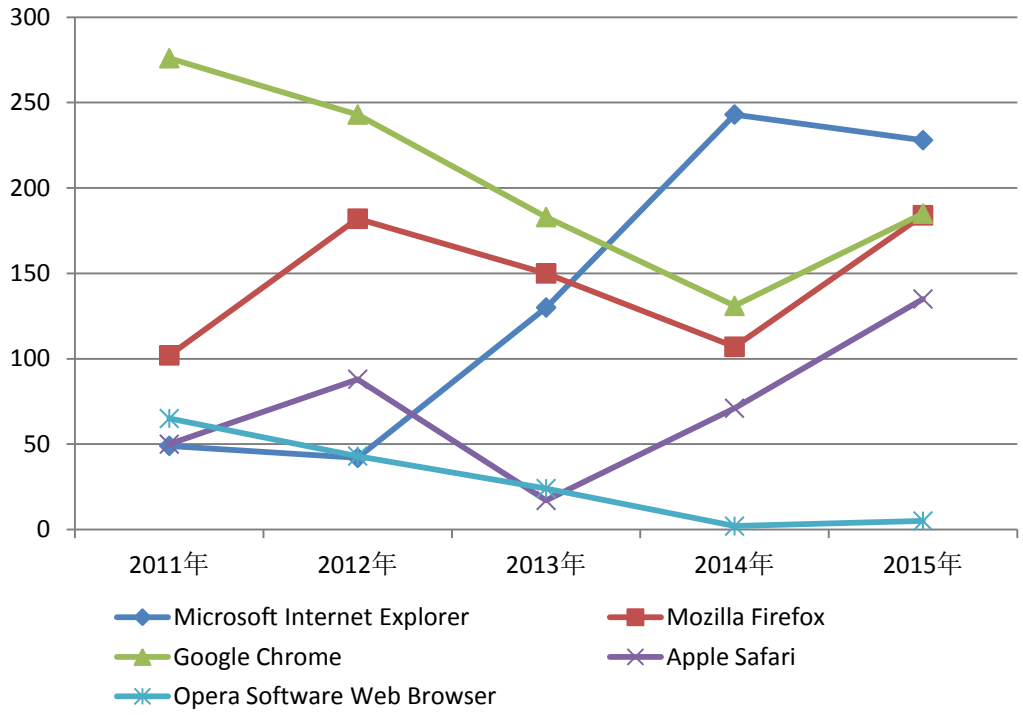

图 10　2011 年至 2015 年主流品牌浏览器漏洞数量年度分布

2.4.3 主流数据库漏洞数据分析

目前市场上数据库产品有 Oracle、SQL Server、MySQL、DB2、Informix、Sybase、Postgresql 等，其中使用较为广泛的数据库有 4 款，分别为：Oracle、SQL Server、MySQL、DB2，这 4 款产品的漏洞数量占据了数据库类产品漏洞总数的 96%以上。因此，我们选取这 4 款产品作为主流数据库产品进行了数据分析。

2015 年共发现主流数据库漏洞 116 个，与 2014 年数据持平。Oracle 公司的两款数据库产品（MySQL 和 Oracle 数据库）的漏洞数量远远高于其他数据库产品，这两款产品分别占到主流数据库漏洞的 66.38%和 25%，合计则达到了 91.38%。DB2 和 SQL Server 两款产品漏洞数量则分别为 7 个和 3 个。

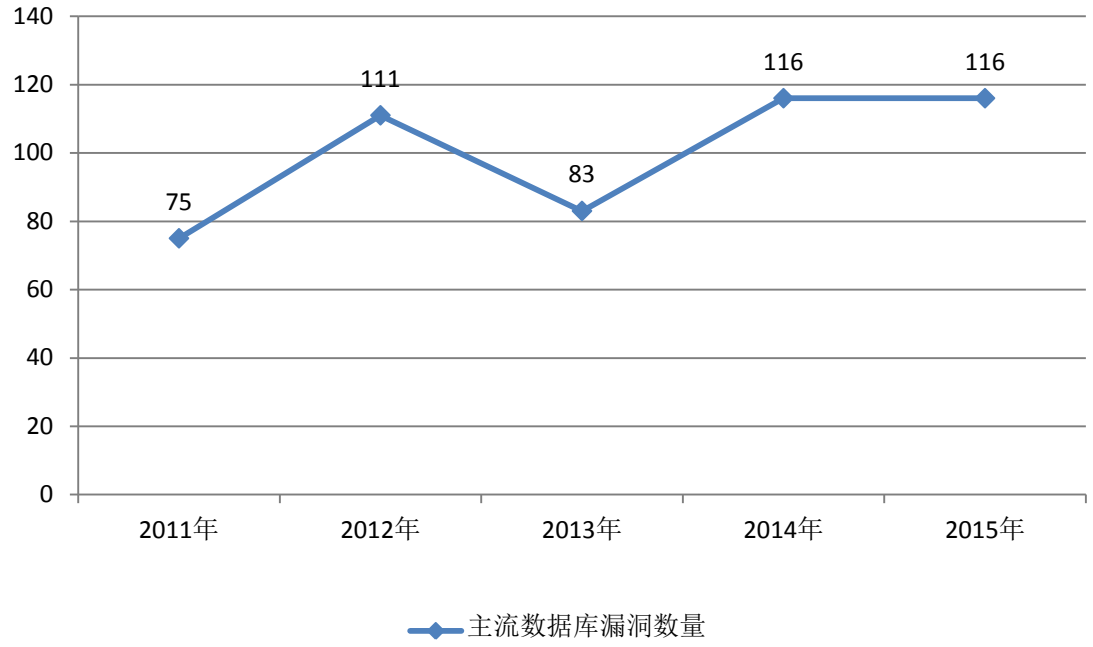

图 11　2011 年至 2015 年主流数据库漏洞数量

（1）主流数据库漏洞年度趋势

2011 年至 2015 年主流数据库漏洞数量如图 11 所示，2011 年漏洞为 75 个，2012 年便跃升至 111 个，增长超过 50%，2013 年数据有较大幅度减少，减少至 83 个，2014 年和 2015 年则趋于平稳，均为 116 个。

（2）主流数据库漏洞分布统计

图 12 展示了 2011 年至 2015 年 4 款主流数据库的漏洞分布情况。从 2012 年 MySQL 漏洞数量超过 Oracle 数据库漏洞数量后，一直占据了数据库漏洞数量的榜首，且近 4 年数量较为平稳，保持在 70 个左右，2015 年数量与上一年相比有了一个小幅度的增加，达到 77 个。Oracle 数据库漏洞数量则出现较大波动：2011 年至 2013 年漏洞数量逐年大幅递减，由 2011 年的 49 个减少到 2012 年的 25 个，降幅达 50%，2013 年继续跌至 13 个，降幅依然达 50%，然而到了 2014 年漏洞数量反弹至 40 个，增幅超过 200%，2015 年又减少近 30%，跌

至 29 个。与前两款产品相比，DB2 和 SQL Server 的漏洞数量由于数量较少，在图中呈现了较为平稳波动的状态。

表 4　2015 年主流数据库漏洞数据

序号	数据库名称	漏洞数量	所占比例
1	MySQL	77	66.38%
2	Oracle	29	25.00%
3	DB2	7	6.03%
4	SQL Server	3	2.59%

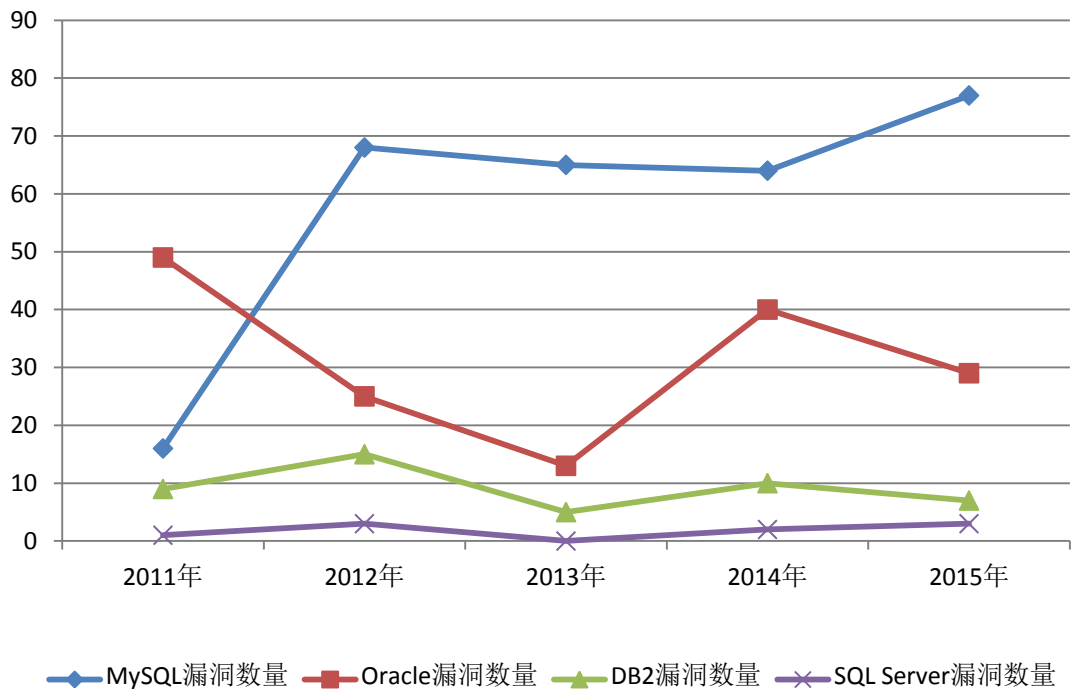

图 12　2011 年至 2015 年主流数据库漏洞数量

三、2015 年重点厂商主要产品漏洞情况

根据重点厂商主要产品的漏洞统计数据，2015 年新增漏洞数量超过 500 个的厂商及组织有 2 家，101-500 个之间的有 6 家，11-100 个之间的有 58 家。新增漏洞数量排名前十的厂商和组织（TOP10 厂商）的相关情况如表 5 所示，这 10 家厂商和组织共出现 3566 个漏洞，占 2015 年新增漏洞数量的 45.99%，排名前 3 的公司漏洞数量总和超过了 20%，排名前 5 的公司漏洞数量总和超过了 30%。这说明 2015 年新增漏洞依然主要集中于各大重点厂商及其主要产品，应作为关注重点。

表 5　2015 年新增漏洞数量 TOP10 厂商情况

序号	厂商名称	2015 年 漏洞数量	2015 年占比	漏洞数量 累计占比
1	Apple	617	7.96%	7.96%
2	Microsoft	535	6.90%	14.86%
3	Cisco	495	6.38%	21.24%
4	Adobe	483	6.23%	27.47%
5	Oracle	477	6.15%	33.62%
6	IBM	315	4.06%	37.68%
7	Google	289	3.73%	41.41%
8	Mozilla	188	2.42%	43.84%
9	HP	88	1.13%	44.97%
10	Linux	79	1.02%	45.99%
合计		3566	45.99%	----

2015 年新增漏洞数量最多的是 Apple 公司，共 617 个，占全年新增漏洞总数的 7.96%；排名第二的是 Microsoft 公司，新增漏洞 535 个；第三名的是 Cisco 公司，新增漏洞 495 个，占全年总数的 6.38%。

与 2014 年相比，新增漏洞数量排名前十的厂商及组织中有 7 家的年度新增漏洞增比上升，增幅最大的是 Adobe 公司，达到了 252.55%，除此之外，Apple 公司产品的漏洞数量也翻了一番，增长了 131.09%；增幅在 0-100%的有 5 家，且大部分增幅集中在 30%-60%，如 Mozilla 组织 59.32%，Microsoft 公司 50.70%，Cisco 公司 34.88%；HP 公司、IBM 公司以及 Linux 组织等 3 家的年度新增漏洞数量下降，幅度分别为-6.38%、-30.16%和-38.28%。

表 6　TOP10 厂商 2015 年增幅排名

序号	厂商名称	2015 年 漏洞数量	2014 年 漏洞数量	2015 年增幅
1	Adobe	483	137	252.55%
2	Apple	617	267	131.09%
3	Google	289	150	92.67%
4	Mozilla	188	118	59.32%
5	Microsoft	535	355	50.70%
6	Cisco	495	367	34.88%
7	Oracle	477	434	9.91%
8	HP	88	94	-6.38%
9	IBM	315	451	-30.16%
10	Linux	79	128	-38.28%
合计		3566	2501	----

如表 7、8 及图 13 所示，TOP10 厂商中，Apple、Oracle、Microsoft、Cisco、Adobe、IBM 等公司的漏洞数量呈现较大幅度的增长；而 Google、Mozilla 、HP、Linux 等公司或组织的漏洞数量呈现小幅波动或略微下降的趋势。Apple 公司一直位于排名的前五名，2015 年该公司相关产品的漏洞数量更是增长了近一倍，由 2014 年排名第 5 直接跃升至首位；Oracle 公司近 5 年连续 3 年占据排名前三的位置， Microsoft 公司 5 次进入前 5 名，排名呈现缓慢上升的趋势，而 Google、HP 等公司的排名近些年来则处于下降的过程。

表 7　TOP10 厂商近 5 年漏洞数量及占比

年份	Apple	Oracle	Microsof	Cisco	Adobe	IBM	Googl	Mozill	HP	Linux
2015	617	477	535	495	483	315	289	188	88	79
	7.96%	6.15%	6.90%	6.38%	6.23%	4.06%	3.73%	2.42%	1.13%	1.02%
2014	267	434	355	367	137	451	150	118	94	128
	3.10%	5.03%	4.12%	4.26%	1.59%	5.23%	1.74%	1.37%	1.09%	1.48%
2013	213	495	362	463	148	386	196	161	137	165
	2.99%	6.95%	5.08%	6.50%	2.08%	5.42%	2.75%	2.26%	1.92%	2.32%
2012	308	380	179	157	148	176	270	203	87	95
	4.28%	5.28%	2.49%	2.18%	2.06%	2.45%	3.75%	2.82%	1.21%	1.32%
2011	254	221	252	167	202	171	296	118	146	130
	4.74%	4.13%	4.71%	3.12%	3.77%	3.19%	5.53%	2.20%	2.73%	2.43%

表 8　2011 至 2015 年漏洞数量最多的十大厂商排名

排名	2011 年	2012 年	2013 年	2014 年	2015 年
1	Google	Oracle	Oracle	IBM	Apple
2	Apple	Apple	Cisco	Oracle	Microsoft
3	Microsoft	Google	IBM	Cisco	Cisco
4	Oracle	Mozilla	Microsoft	Microsoft	Adobe
5	Adobe	Microsoft	Apple	Apple	Oracle
6	IBM	IBM	Google	Google	IBM
7	Cisco	Cisco	Linux	Adobe	Google
8	HP	Adobe	Mozilla	Linux	Mozilla
9	Linux	Linux	Adobe	Mozilla	HP
10	Mozilla	HP	HP	HP	Linux
占比	36.55%	27.83%	38.26%	29.00%	45.99%

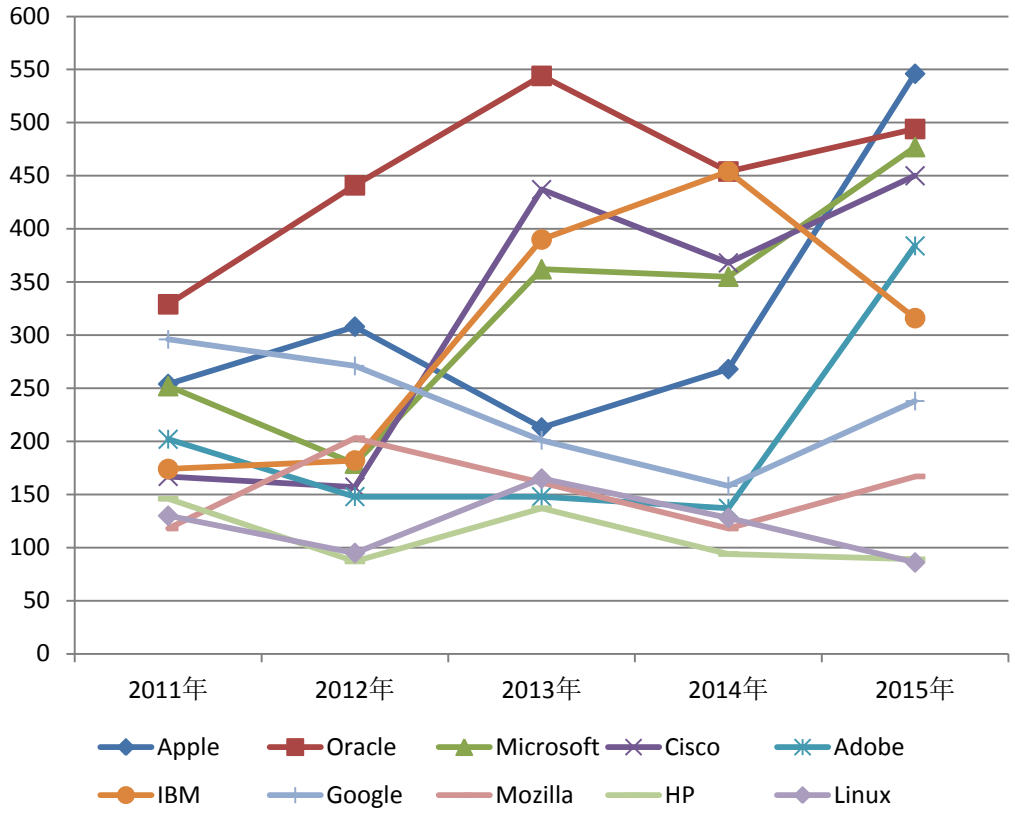

图 13　TOP10 厂商近 5 年漏洞数量趋势图

下面分别对 2015 年重点厂商主要产品漏洞的具体情况进行分析，主要包括 Apple、Oracle、Microsoft、Cisco、Adobe、Google 等重点厂商的主要信息技术产品。

3.1 Apple 公司主要产品漏洞数据分析

Apple 公司软件产品主要包括 iOS 操作系统、Mac OS X 操作系统、Safari 浏览器、iTunes 数字媒体播放应用程序、QuickTime 媒体播放器、iWork 办公软件、iCloud 私有云空间、AppStore 软件销售平台等，其中 iOS、Mac OS X、Safari、iTunes 和 QuickTime 等五款主要产品漏洞数量较多，占据 Apple 公司漏洞总数的 90%以上，尤其是 iOS 和 Mac OS X 漏洞数量常年居高不下，是 Apple 公司中漏洞所占比重最大的两款产品。

2015 年 Apple 公司新增漏洞数量为 617 个，其中多款 Apple 产品通用的漏洞占有很大比重。2015 年 Apple 公司五大产品新增安全漏洞如表 9 所示，其中 iOS 和 Mac OS X 系统漏洞数量最多，分别达到 375 个和 359 个，占 Apple 漏洞总数的 60.78%和 58.18%，其中有 136 个漏洞同时影响 iOS 和 Mac OS X 系统。Safari 浏览器的漏洞数量也出现明显增长，达到 135 个，部分漏洞同时影响 Mac OS X 和 Safari。iTunes 漏洞数量也较多，共 100 个。此外 Apple 公司其他产品，如 QuickTime、iCloud 等，漏洞数量都较少。

Apple 公司在企业用户市场的发力初见成效，2015 年 9 月 Apple 新设备的发布会也带来了其市场份额的上升，Apple 设备越来越多地成为市场的主流产品，IBM 也在帮助 Apple 更好地将旗下产品应用于企业市场。目前 iOS 系统的企业市场份额已达到 60%以上；而随着 Mac 计算机逐渐普及，Apple 公司在 PC 市场也于 2015 年第三季度跃居全球第四大 PC 厂商；Safari 浏览器的市场份额也出现小幅度提升。市场份额的增加、产品关注度的提升、用户数量的增长，使得 Apple 公司产品漏洞成为黑客关注的热点，其产品安全也成为当前研究的重点。

表 9　2015 年 Apple 公司主要产品新增安全漏洞统计表

序号	产品名称	漏洞数量	所占比例
1	iOS	375	60.78%
2	Mac OS X	359	58.18%
3	Safari	135	21.88%
4	iTunes	100	16.21%
5	QuickTime	22	3.57%

3.1.1 iOS 漏洞数据分析

iOS 是 Apple 公司最早为 iPhone 设计的移动操作系统，后来陆续套用到 iPod touch、iPad 以及 Apple TV 等产品上。根据 2011 年至 2015 年 iOS 操作系统漏洞数量统计图，iOS 漏洞数量整体呈上升趋势。2010 年 Apple 公司将“iPhone OS”改名为“iOS”，2011 年 iOS 系统市场份额开始增长，当年 iOS 漏洞共 36 个，2012 年 iPhone 4S 发布，Apple 公司推出了新一代 iPad，导致 2012 年漏洞上升至 112 个，2012 至 2014 年漏洞数量较为平均，均在 100 个左右，直到 2015 年跃升为 375 个，达到近年最大值，相当于前四年漏洞数量的总和。iOS 系统漏洞在 Apple 公司漏洞总数中的占比也是逐年增加，从 2011 年的 14.17%上升至 2015 年的 60.78%。随着 iOS 系统的产品迅速普及以及 iOS 设备在企业市场的推广，安全研究人员对于 iOS 系统的关注热情迅速增长。

值得一提的是，国内涌现出了盘古、太极等针对 Mac OS X 和 iOS 系统进行漏洞研究的专业团队，其漏洞分析的技术能力非常突出。

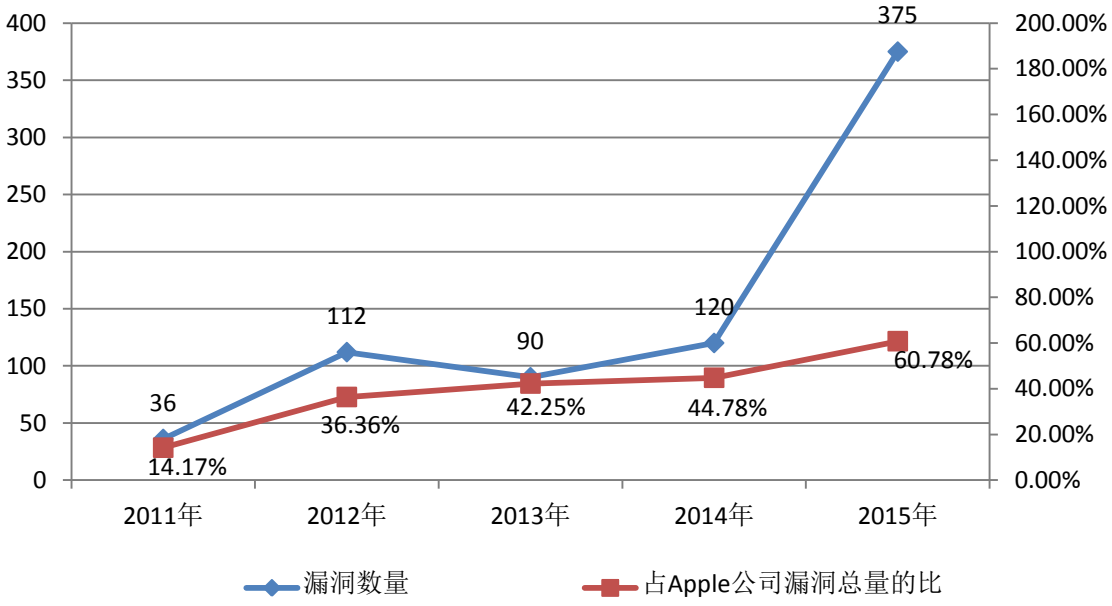

图 14　2011 年至 2015 年 iOS 操作系统漏洞数量统计图

3.1.2 Mac OS X 漏洞数据分析

Mac OS X 是 Apple 公司为 Mac 系列产品开发的专属操作系统，随着 Mac 系列产品市场份额的增长，Mac OS X 也曝出了越来越多的漏洞。根据 2011 年至 2015 年 Mac OS X 操作系统漏洞数量统计图，Mac OS X 漏洞数量除在 2012 年稍有减少之外，整体呈上升趋势。2011 年 Apple 发布 Mac OS X 10.7，引入了更多 iOS 的特性，沿用多年的 Mac OS X 改用“线上发售+下载”的形式进行销售，当年漏洞达到 72 个，占 Apple 公司漏洞的 28.35%。2012 年推出的 Mac OS X 10.8 Mountain Lion，大幅度改进了其安全性，当年漏洞减少到 35 个。2013 年起，随着 Mac OS X 市场占有率的飞速增长，Mac OS X 漏洞逐年上升，2015 年增长至 359 个，占 Apple 公司漏洞的 58.18%，相当于近四年漏洞数量的总和。

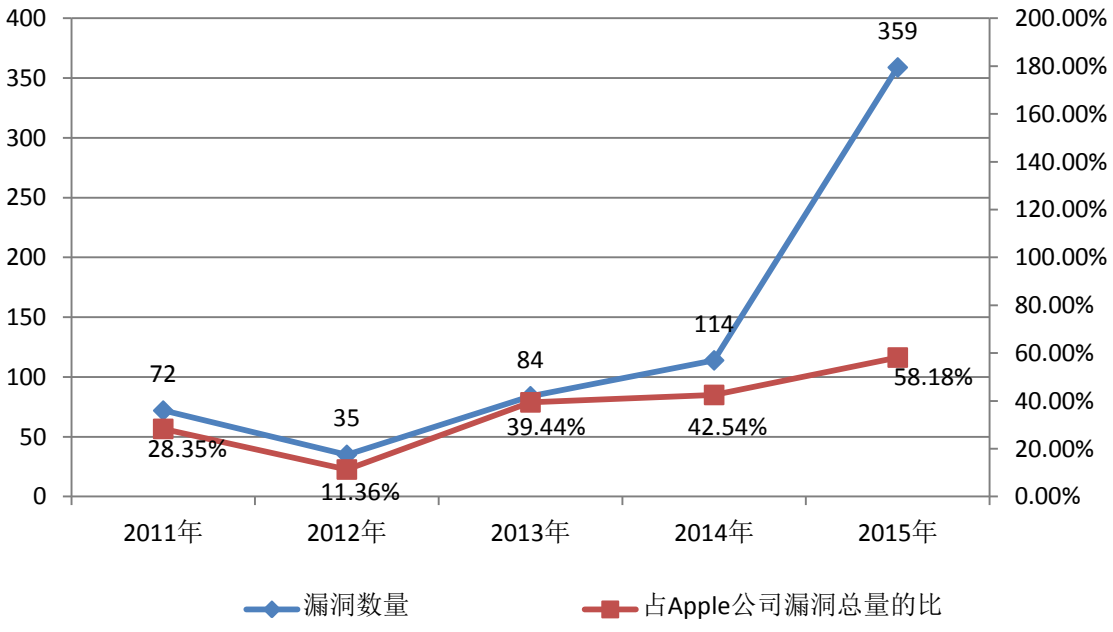

图 15　2011 年至 2015 年 Mac OS X 操作系统漏洞数量统计图

3.1.3 Safari 漏洞数据分析

Safari 是 Mac OS X 操作系统中的浏览器，也是 iPhone、iPodTouch、iPad 中 iOS 的默认浏览器。2011 年至 2015 年，Safari 漏洞平均每年 72 个，2013 年 Safari 漏洞数量达到最低值，仅 17 个，占 Apple 公司漏洞数量的 7.98%，除了 2013 年之外，Safari 漏洞基本上占据 Apple 公司漏洞总数的 20%，是除 iOS、Mac OS X 之外漏洞数量最多的产品，2013 年之后，Safari 漏洞数量大幅度提升，平均每年增加 59 个，2015 年达到最多的 135 个。

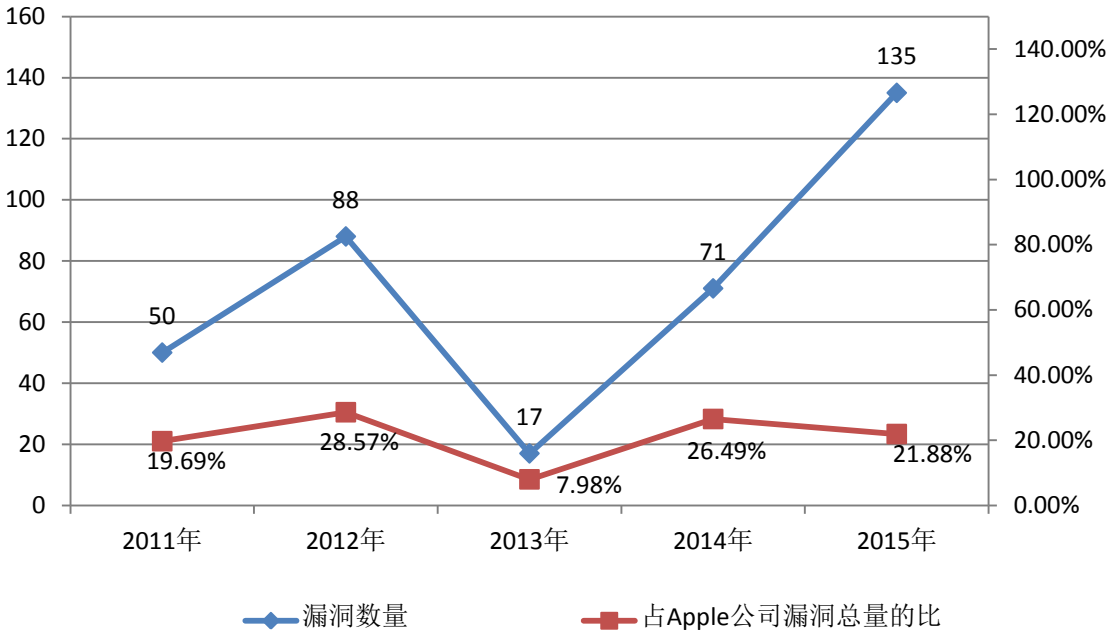

图 16　2011 年至 2015 年 Safari 漏洞数量统计图

3.1.4 iTunes 漏洞数据分析

iTunes 是一款数字媒体播放应用程序，是供 Mac 和 PC 使用的一款免费应用软件，能管理和播放数字音乐和视频。2011 年和 2012 年 iTunes 漏洞数量较高，甚至高于 iOS、Mac OS X 和 Safari，达到 78 个和 111 个，占 Apple 公司漏洞数量的 30%以上。2013 年 Apple 开始为“Apple ID”账号提供两步认证安全

选项，用户利用持有终端通过“iTunes”、“App Store”和“iBookstore”等购买内容或是管理账号信息时，除密码外，还需要输入发送到终端上的 4 位数验证码，极大地提升了安全性，2013 年 iTunes 漏洞数量突降至 23 个，2014 年继续减少至 13 个。直到 2015 年，随着 Mac 市场占有率的不断提升，针对 iTunes 的研究逐渐成为热点，iTunes 漏洞数量上升至 100 个，占 Apple 公司漏洞总量的 16.21%。

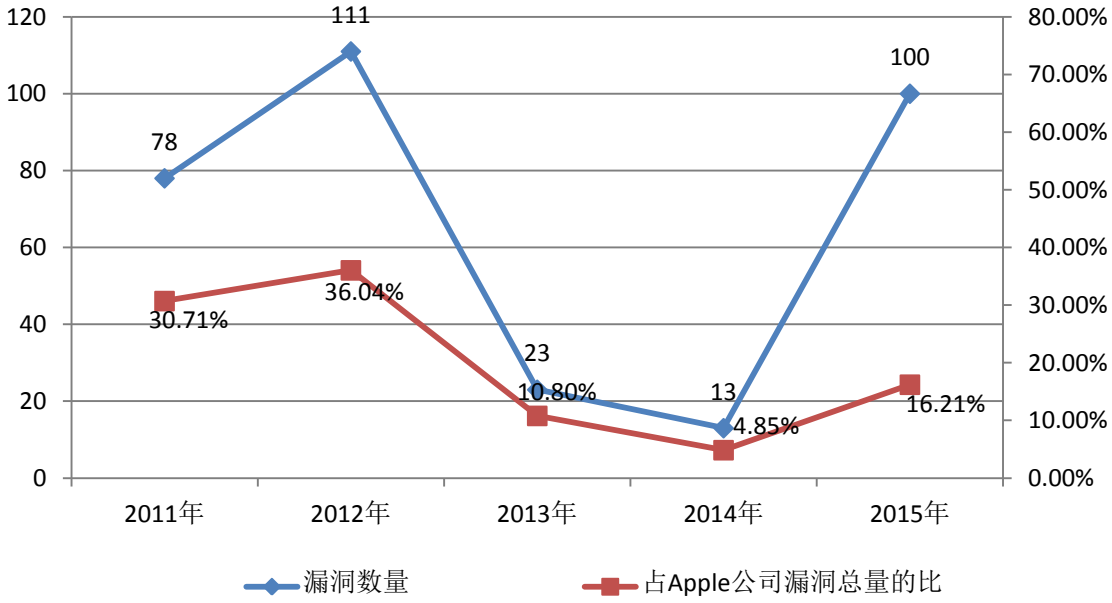

图 17　2011 年至 2015 年 iTunes 漏洞数量统计图

3.1.5 QuickTime 漏洞数据分析

QuickTime 是一款跨平台的多媒体播放器，可以运行在 Mac OS X 和 Windows 系统上。根据 2011 至 2015 年 QuickTime 产品漏洞统计表，QuickTime 漏洞数量最高时是 2011 年和 2015 年的 22 个，最低为 2014 年的 10 个，QuickTime 平均每年曝出 17 个漏洞，在 Apple 公司产品漏洞数量排名第五。2011 年至 2014 年 QuickTime 漏洞数量逐年减少，2015 年虽有上升，达到 2014 年的两倍，共 22 个，但在 Apple 公司漏洞的占比仍旧较低，仅为 3.57%。QuickTime

漏洞占 Apple 公司的漏洞总量的百分比最高时是 2011 年，比例为 8.66%，并且呈现逐年降低的趋势。

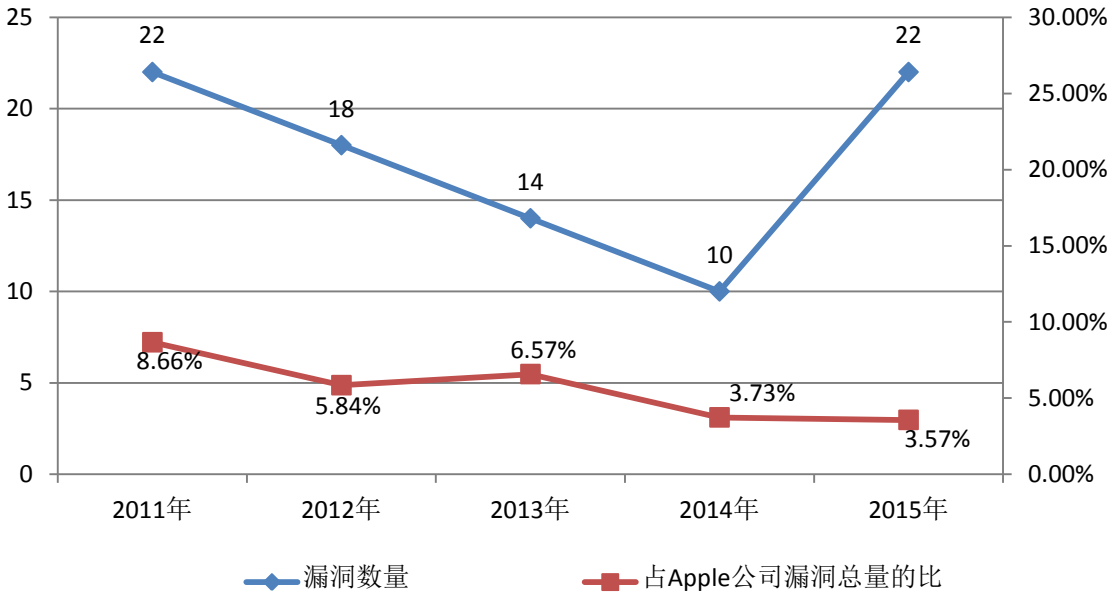

图 18　2011 年至 2015 年 QuickTime 漏洞数量统计图

3.2 Oracle 公司主要产品漏洞数据分析

Oracle 公司软件产品主要包括 Java 平台（JRE、JDK、JRockit 等）、企业应用软件（ERP、CRM 等）、Oracle 数据库、MySQL 数据库、Java DB 数据库、Berkeley DB 数据库、Fusion Middleware 中间件、Solaris 操作系统、Oracle Linux 操作系统、Oracle VM 虚拟技术、VirtualBox 虚拟技术等，其中 Java 平台、MySQL、Fusion Middleware、Oracle 企业应用软件和 Oracle 数据库等五款主要产品漏洞数量较多，占 Oracle 公司漏洞总量的 66.25%。

2015 年 Oracle 公司新增漏洞数量为 477 个，2015 年 Oracle 公司五大产品新增安全漏洞如表 10 所示，其中 Java 平台漏洞数量最多，共有 80 个，占 Oracle 公司漏洞总量的 16.77%，MySQL 的漏洞数量也达到 77 个，占 Oracle 公司漏洞总量的 16.14%。Fusion Middleware 中间件产品、Oracle 企业应用软件的漏

洞数量也呈现出上升趋势，与上述产品相反，Oracle 数据库的漏洞数量呈现出下降趋势。

Oracle 公司自 2002 年起进军中国的企业应用市场，中国制造、银行和证券、保险、医疗卫生、教育、政府、交通运输、物流、零售、公用事业以及专业服务行业的中型企业越来越多地采用了 Oracle 数据库和 Oracle 融合中间件。Oracle 数据库占据全球最大的市场份额，集成平台、融合中间件、企业应用软件等市场份额也逐步加大，Oracle 公司的产品越来越多的被安全研究人员关注，产品漏洞数量越来越多。

表 10　2015 年 Oracle 公司主要产品新增安全漏洞统计表

序号	产品名称	漏洞数量	所占比例
1	Java 平台	80	16.77%
2	MySQL	77	16.14%
3	Fusion Middleware	67	14.05%
4	Oracle 企业应用软件	63	13.21%
5	Oracle 数据库	29	6.08%

3.2.1 Java 平台漏洞数据分析

Java 是一种可以撰写跨平台应用软件的面向对象的程序设计语言，广泛应用于个人 PC、数据中心、游戏控制台、科学超级计算机、移动电话和互联网，同时拥有全球最大的开发者专业社群，故而 Oracle 公司产品中 Java 平台漏洞数量最多，同时影响范围也相对较广。Java 平台漏洞数量波动较大，平均每年 87 个。2011 年 Java 平台漏洞数量仅 3 个，在 2012 和 2013 年出现迅猛增长，2013 年达到近五年最大值 180 个，占 Oracle 公司漏洞总数的 35.71%，2014 年漏洞

数量开始减少，降低至 115 个，2015 年继续减少，仅为 80 个，占 Oracle 公司漏洞总数的 16.77%。

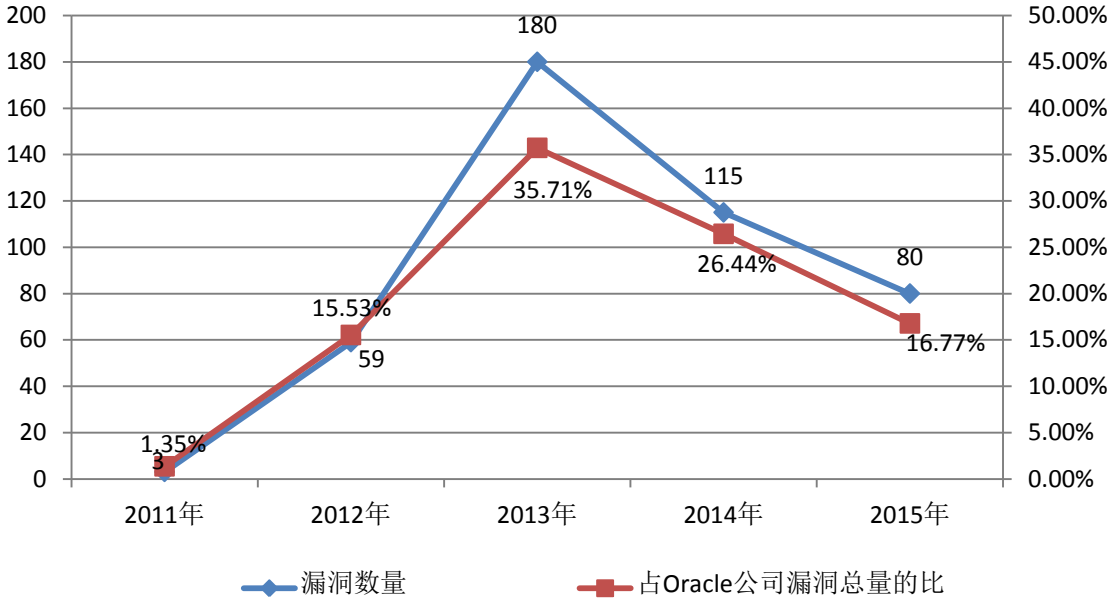

图 19　2011 年至 2015 年 Java 平台漏洞数量统计图

3.2.2 MySQL 漏洞数据分析

MySQL 数据库体积小、速度快、并且开放了源代码，许多中小型网站为了降低网站总体拥有成本而选择其作为网站数据库，除 2011 年之外 MySQL 每年漏洞数量均在 60 个以上，占 Oracle 公司漏洞数量的比也均在 10%以上，2012 年、2013 年和 2014 年 MySQL 漏洞数量均为 65 个上下，2015 年出现明显上升，达到 77 个，占 Oracle 公司漏洞总数的 16.14%，排名第二。

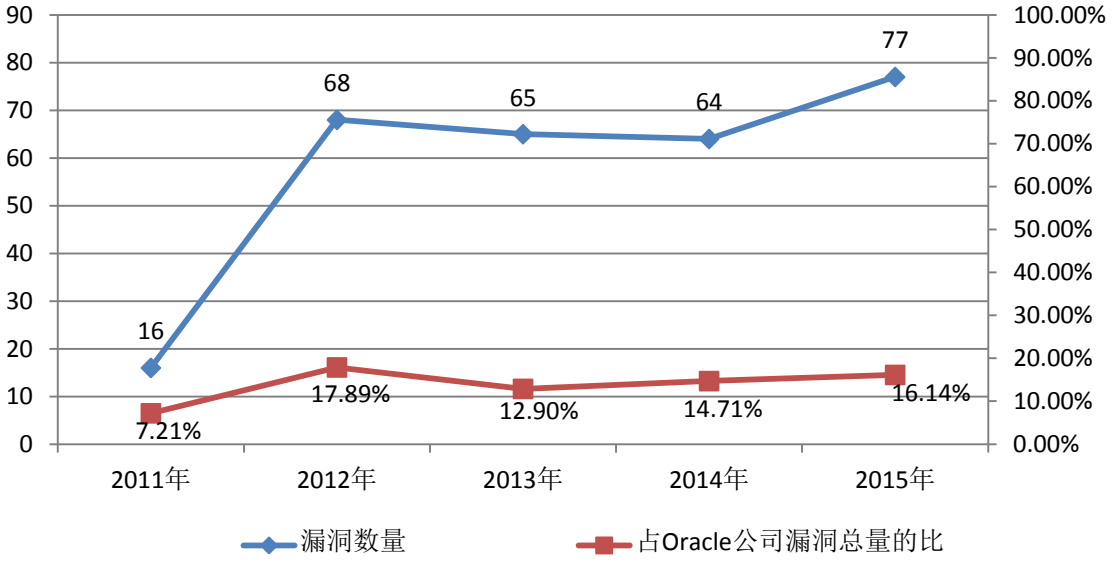

图 20　2011 年至 2015 年 MySQL 漏洞数量统计图

3.2.3 Fusion Middleware 漏洞数据分析

Oracle 公司的中间件产品在全球占有率颇高，Fusion Middleware 等产品的漏洞也成为需要关注的重点。2011 年至 2015 年 Fusion Middleware 产品漏洞数量统计如图 21 所示，Fusion Middleware 产品漏洞与 Java 平台呈现出相反的增长趋势，2011 年 Fusion Middleware 漏洞数量为 36 个，2012 年呈现小幅度增长，升至 64 个，2013 年大幅度下降，漏洞仅 40 个，2014 年开始漏洞数量不断上升，达到 58 个，2015 年更是升至 67 个，占 Oracle 公司漏洞总量的 14.05%，排名第三。

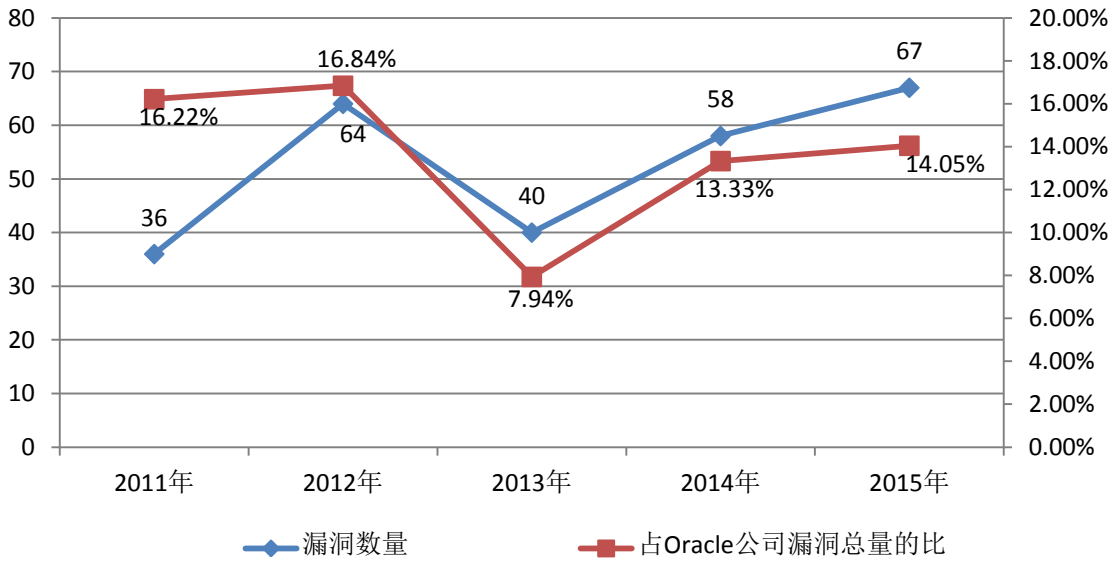

图 21　2011 年至 2015 年 Fusion Middleware 漏洞数量统计图

3.2.4 Oracle 企业应用软件漏洞数据分析

Oracle 公司是全球最大的企业级软件公司，Oracle 企业应用软件包括 Siebel CRM、E-Business Suite、JD Edwards EnterpriseOne、PeopleSoft 系列等多种软件，是 Oracle 公司近几年重点发展的产品。2011 年 Oracle 企业应用软件漏洞数量仅为 40 个，2012 年开始增长，达到 59 个，2013 年增长平缓，数量为 60 个，2014 年出现小幅度下降，降至 53 个，2015 年上升至近五年最大值，即 63 个，占 Oracle 公司漏洞总量的 13.21%。

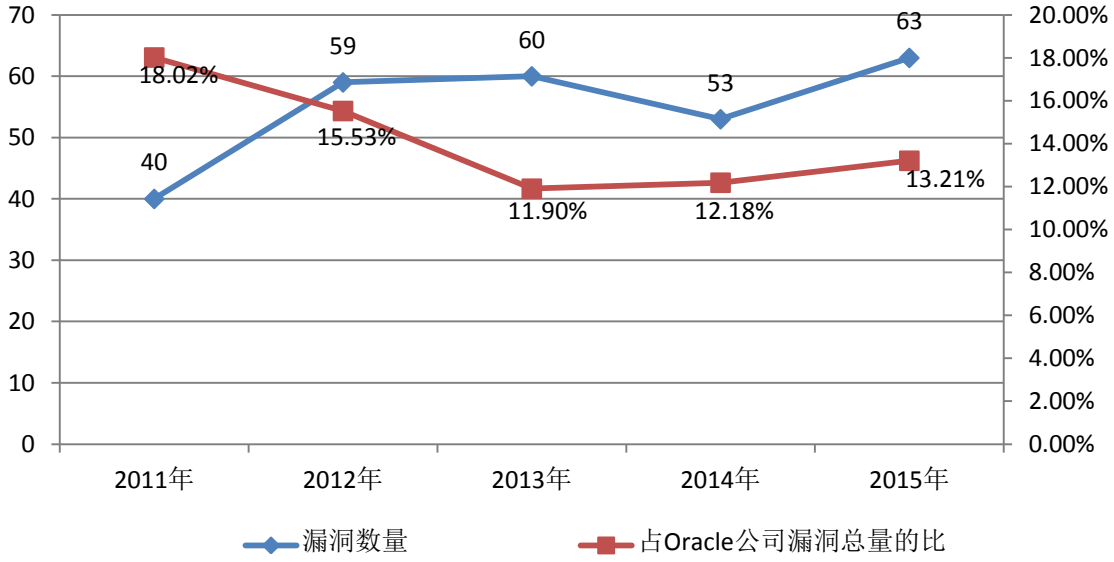

图 22　2011 年至 2015 年 Oracle 企业应用软件漏洞数量统计图

3.2.5 Oracle 数据库漏洞数据分析

Oracle 公司的数据库产品中，除了 MySQL 之外，Oracle 漏洞数量也占据了较大比重。2011 年 Oracle 漏洞为 49 个，占 Oracle 公司漏洞总量的 22.07%，2012 年大幅度下降，仅 25 个，2013 年继续减少，达到近五年最低值 13 个，仅占 Oracle 公司漏洞总量的 2.58%，2014 年漏洞数量大幅度回升，升至 40 个，2015 年减少至 29 个，占 Oracle 公司漏洞总量的 6.08%。

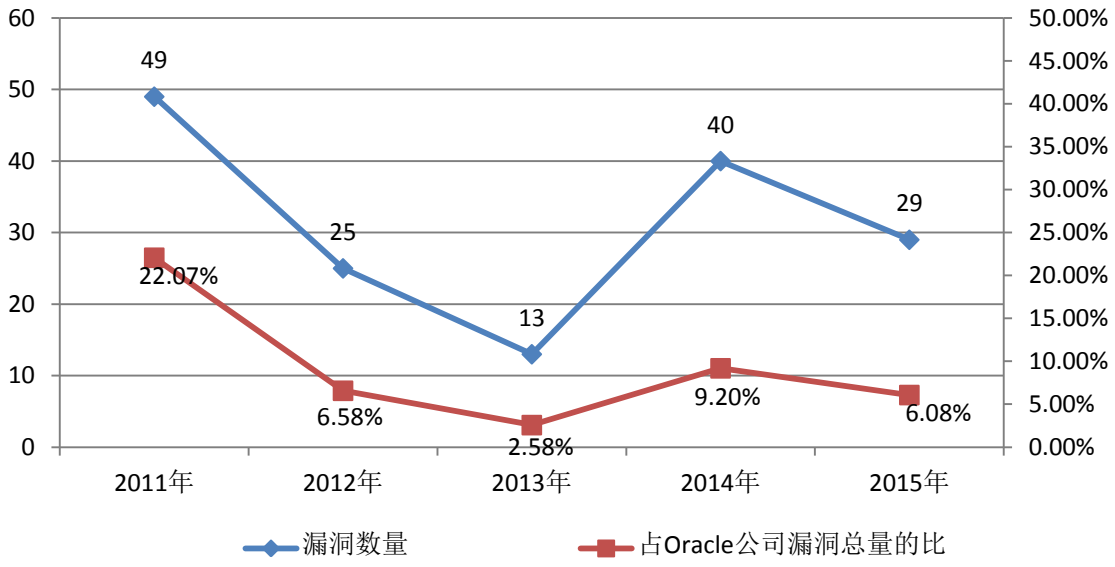

图 23　2011 年至 2015 年 Oracle 数据库产品漏洞数量统计图

3.3 Microsoft 公司主要产品漏洞数据分析

Microsoft 公司目前是全球最著名的计算机软件提供商之一，其在全球市场上的主要产品有 Microsoft Windows 系列操作系统、Microsoft Office（Word、Excel、Outlook、PowerPoint）系列软件、Visual Studio 集成开发环境、IE 浏览器、Windows Media Player 播放器、MSDN 系列软件等，其中 Microsoft Windows 系列操作系统包括桌面操作系统 Windows Vista、Windows 7、Windows 8、Windows 10、Windows RT 以及服务器操作系统 Windows Sever 2008、2012 等。

2015 年，该公司的主要产品共发现漏洞 535 个，在所有厂商中排名第 2，漏洞数量比去年增加 180 个，增幅为 33.64%，IE 浏览器、Windows Server 系列、Windows 系列、Office 等主要产品的漏洞占据 Microsoft 公司漏洞总数的 95%以上，其中 Windows 操作系统多款产品通用的漏洞较多。由 2015 年 Microsoft 公司主要产品新增安全漏洞统计表可以看出，IE 浏览器漏洞数量最多，全年新增漏洞 228 个，占该公司全新新增漏洞总数的 42.62%；Windows Server

系列紧随其后，共发现漏洞 171 个，占全新新增漏洞总数的 31.96%；排名第三的是 Windows 系列，共发现漏洞 169 个，占全年新增漏洞总数的 31.59%。微软主要产品除 IE 浏览器的漏洞数量增幅有所减少以外，其余几类产品的漏洞数量增幅均超过 100%。其中，Windows Server 和 Windows 系列两个系列增幅甚至接近 300%，而且这几款产品 2015 年新增的漏洞数量均为近 5 年来年度漏洞新增数量的最大值。

表 11　2015 年 Microsoft 公司主要产品新增安全漏洞统计表

序号	产品名称	类型	漏洞数量	所占比例
1	IE	浏览器	228	42.62%
2	Windows Server 系列	服务器操作系统	171	31.96%
3	Windows 系列	桌面操作系统	169	31.59%
4	Office 系列	办公软件	79	14.77%
5	Windows 10	桌面操作系统	45	9.43%

3.3.1 IE 漏洞数据分析

IE 浏览器即 Internet Explorer，是 Microsoft 公司于 1994 年推出的一款网页浏览器，目前最新版本为 IE 11，于 2013 年 10 月 17 日正式发布。虽然 2015 年 3 月，Microsoft 公司确认将放弃 IE 品牌，并在 Windows 10 版本中以 Microsoft Edge 取代目前的 IE 浏览器，并于 2015 年 10 月宣布自 2016 年 1 月起停止对 IE 浏览器的支持，但由于 IE 浏览器已开发运行了 21 个年头，且目前仍在主流浏览器中占据大量市场份额，所以 IE 浏览器依然是全球范围内漏洞挖掘研究的

重要目标。该产品 2015 年新增漏洞数量为 200 个，不仅是 Microsoft 公司所有产品中数量最多的，也是市场主流浏览器中数量最多的。究其原因，漏洞挖掘组织和个人的高度关注和产品本身的安全性问题都是重要因素，这也促使 Microsoft 公司加速对新浏览器 Microsoft Edge 的推广。

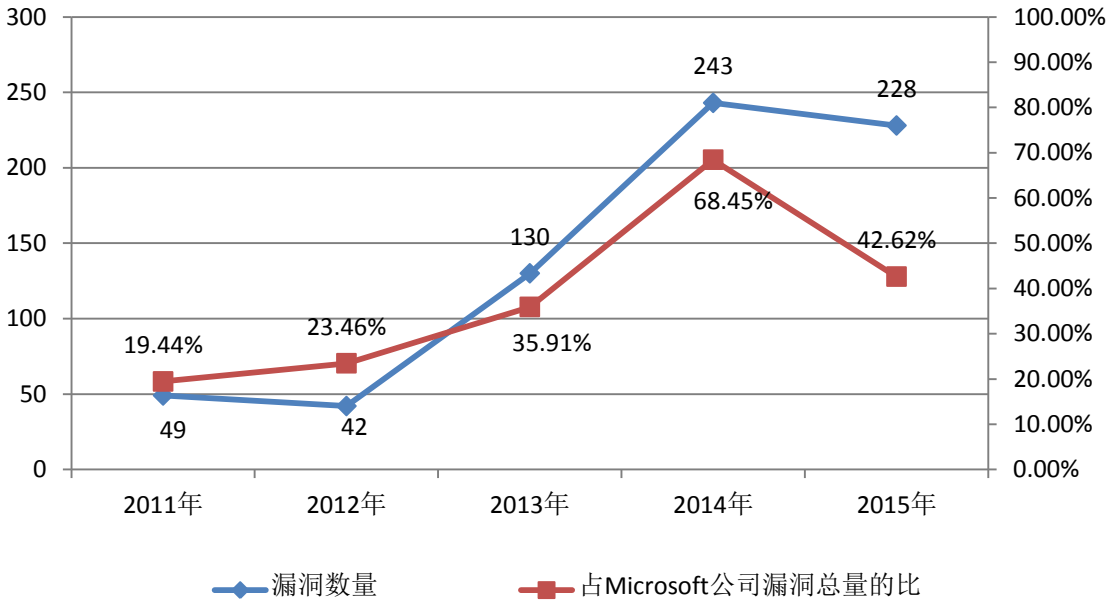

图 24　2011 年至 2015 年 IE 浏览器漏洞数量统计图

如 2011 年至 2015 年 IE 浏览器漏洞数量统计图所示，自 2011 年起，IE 浏览器漏洞数量整体呈现大幅增长的态势，虽然 2011 年和 2012 年漏洞数量较为平稳，但 2013 年至 2014 年的迅速增长，全年新增漏洞数量飙升至 243 个，两年间增幅达到 4 倍多，也使得 2014 年成为近 5 年来 IE 浏览器新增漏洞数量最多的一年；2015 年数量有所回落，全年新增数量比 2014 年减少了 15 个，降幅为 6.17%，出现这一情况有可能是因为 Microsoft 公司于 2015 年下半年新推出了新浏览器 Microsoft Edge，从而分散了一部分漏洞挖掘组织和个人的注意力，进而使得漏洞数量有所减少。

3.3.2 Windows Server 系列漏洞数据分析

Windows Server 系列是 Microsoft 公司发布的服务器操作系统，主要版本有 Windows Server 2003、2008、2012，Microsoft 公司将于 2016 年发布 Windows Server 2016。根据 2011 年至 2015 年 Windows Server 系列操作系统漏洞数量统计，近 5 年该产品的漏洞每年新增数量均有较大波动，如 2011 全年年新增漏洞数量 114 个，2012 年则跌至 56 个，跌幅接近 50%，2013 年大幅反弹至 108 个，2014 年则大幅减少至 41 个，这也是近 5 年该系列产品新增漏洞数量最少的一年。2015 年，Windows Server 系列产品一共发现了 171 个漏洞，和前一年相比增幅高达 317.07%，也使 2015 年成为近 5 年该系列产品漏洞增长最多的一年。

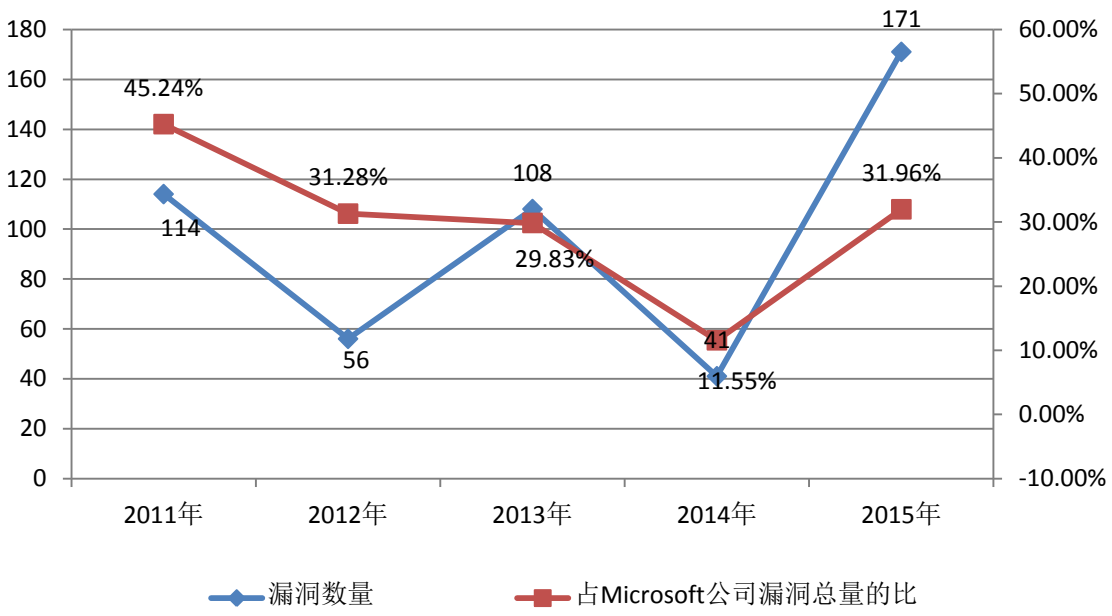

图 25　2011 年至 2015 年 Windows Server 系列漏洞数量统计图

3.3.3 Windows 系列漏洞数据分析

Microsoft Windows 是 Microsoft 公司研发的一套桌面操作系统，它问世于 1985 年 11 月 20 日，在 30 年的不断改进和发展中，该系列产品一直具有极高

的操作系统市场占有率。目前该系列产品主要有 Windows Vista、Windows 7、Windows 8 以及 Windows10。

由 2011 年至 2015 年 Windows 系列漏洞数量统计图我们可以看出，该系列产品漏洞数量与 Windows Server 系列十分相似，近 5 年来呈现“W”型走势，新增漏洞数量从 2011 年的 116 个跌至 2012 年的 56 个，2013 年增加近 100%至 111 个，随后在 2014 年跌至近 5 年最低点。2015 年该系列产品漏洞数量增幅达 312.20%。2014 年年中发布的 Windows 8.1 Spring Update 并没有显著提高 Windows 桌面操作系统系列的安全性，相反，2015 年共发现该版本漏洞 141 个，成为该系列产品 2015 年漏洞数量最多的一个版本。

2015 年 7 月 29 日，Microsoft 公司正式发布了 Window 10 系统， 2015 年 CNNVD 收录该系统漏洞 45 个，平均每月 9 个。CNNVD 收录的该系统第一个漏洞是在 2015 年 8 月 13 日，漏洞名称为“Microsoft Windows Mount Manager 特权提升漏洞”（编号 CNNVD-201508-135），属于高危漏洞。

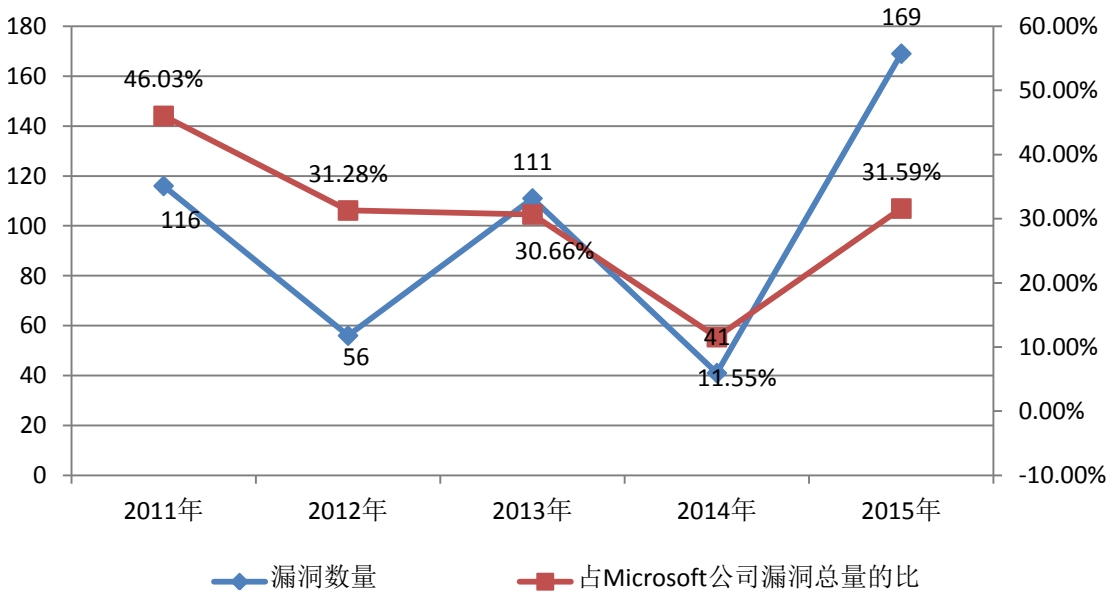

图 26　2011 年至 2015 年 Windows 系列漏洞数量统计图

3.3.4 Office 系列漏洞数据分析

Microsoft Office 是 Microsoft 公司公司开发的一套基于 Windows 操作系统的办公软件套装。常用组件有 Word、Excel、PowerPoint 等。最新版本为 Office 365(Office 2016)。

由 2011 年至 2015 年 Office 系列漏洞数量统计图我们可以看出 2011 年至 2013 年这 3 年 Office 系列产品每年新增漏洞数量稳定在 50 个左右，2014 年下降 72.73%至 33 个，而 2015 年，Office 漏洞数量增长接近 140%，达到 5 年来最高值 79 个。

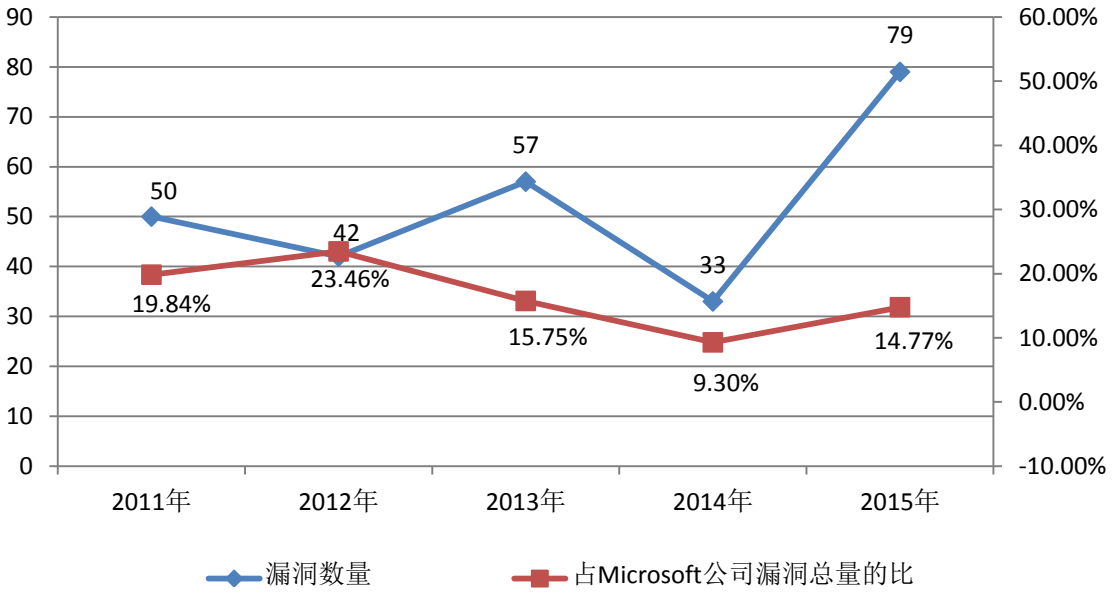

图 27　2011 年至 2015 年 Office 系列漏洞数量统计图

3.4 Cisco 公司主要产品漏洞数据分析

Cisco 公司产品主要有路由器（800、7600、ASR9000、CRS-1 等）、交换机（Catalyst 系列、Nexus 系列等）、防火墙（PIX、ASA 等）、IOS 网络操作系统、NX-OS 网络交换机操作系统、WebEx 网络会议软件、TelePresence 网真视频通信服务器等。2015 年 Cisco 公司新增的漏洞数量为 495 个，涉及产

品众多，达到 135 款产品，平均每款产品漏洞数量为 3 个。其中，IOS、NX-OS、WebEx、TelePresence、ASA 这五款主要产品漏洞数量较多，占 Cisco 漏洞总量的 34%，所以下面主要针对上述五款产品进行重点分析。

2015 年 Cisco 公司五大产品新增安全漏洞如表 12 所示，其中 IOS 漏洞数量最多，达到 85 个，占 Cisco 公司漏洞总量的 17.17%，TelePresence 漏洞数量排名第二，共 58 个，占 Cisco 公司漏洞总量的 11.72%。此外，WebEx、NX-OS 和 ASA 漏洞数量相当，均在 20 个以上。近些年 Cisco 公司漏洞数量逐年升高，然而 ASA 产品漏洞数量呈现整体下降的趋势。

表 12　2015 年 Cisco 公司主要产品新增安全漏洞统计表

序号	产品名称	漏洞数量	所占比例
1	IOS	85	17.17%
2	TelePresence	58	11.72%
3	WebEx	29	5.86%
4	NX-OS	22	4.44%
5	ASA	20	4.04%

3.4.1 IOS 漏洞数据分析

Cisco 公司路由器和交换机产品在全球市场中占有重要份额，因此其路由器和交换机的安全漏洞和问题隐患也吸引着全球安全研究人员和黑客的目光。IOS 是多款 Cisco 路由器设备中使用的操作系统，也是 Cisco 公司漏洞数量最多的产品，平均每年达到 62 个。2011 年至 2015 年 IOS 产品漏洞数量统计如图 28 所示，2011 年数量为 44 个，漏洞数量呈现逐年上升的趋势，平均每年增加 7 个漏洞，到 2015 年达到 85 个，可见 IOS 的漏洞数量呈现出继续增长的明显趋势。

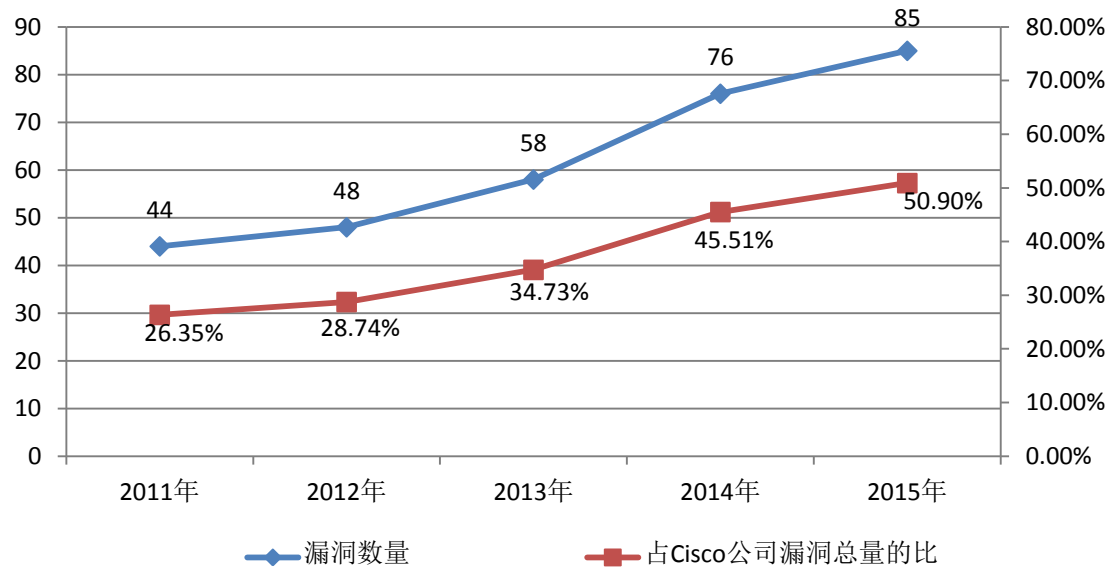

图 28　2011 年至 2015 年 IOS 产品漏洞数量统计图

3.4.2 TelePresence 产品漏洞数据分析

TelePresence 是 Cisco 公司的一套被称为“网真”系统的视频会议解决方案，该方案提供音频、视频空间等组件，可为远程参会者提供一个“面对面”的虚拟会议室效果。根据 2011 年至 2015 年 TelePresence 产品漏洞数量统计可知，TelePresence 漏洞数量波动较为明显，2011 年漏洞数量 41 个，2012 年减少到最低，仅 14 个，2013 年起开始呈现逐年增长的趋势，当年增长至 20 个，2014 年继续大幅度上升，漏洞数量达到 44 个，2015 年升至最高，达到 58 个，占 Oracle 公司漏洞总量的 11.72%。虽然 TelePresence 漏洞数量呈整体上升趋势，但是其占 Cisco 漏洞总量的比例是呈现下降趋势，可见越来越多的 Cisco 公司产品开始受到安全研究人员和黑客的关注。

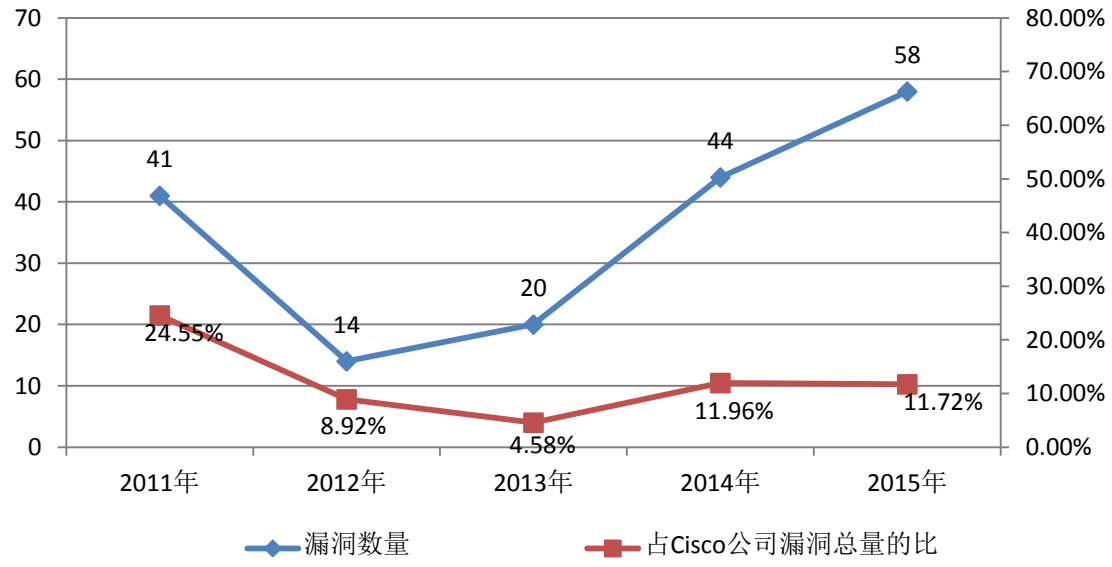

图 29　2011 年至 2015 年 TelePresence 产品漏洞数量统计图

3.4.3 WebEx 产品漏洞数据分析

WebEx 是 Cisco 公司的一套 Web 会议工具，该工具可协助异地办公人员进行协调合作。WebEx 服务包括 Web 会议、网真视频会议和企业即时消息(IM)等。与 TelePresence 产品相同，WebEx 也是 Cisco 公司一款重要的企业应用产品。根据 2011 年至 2015 年 WebEx 产品漏洞数量统计图所示，WebEx 漏洞数量呈整体上升趋势，从 2011 年的 13 个，2012 年稍有下降，为 11 个，2013 年大幅度上升至最大值 41 个，2014 年开始逐年小幅度下降，平均每年减少 6 个，2015 年降至 29 个，占 Oracle 公司漏洞总量的 5.86%。

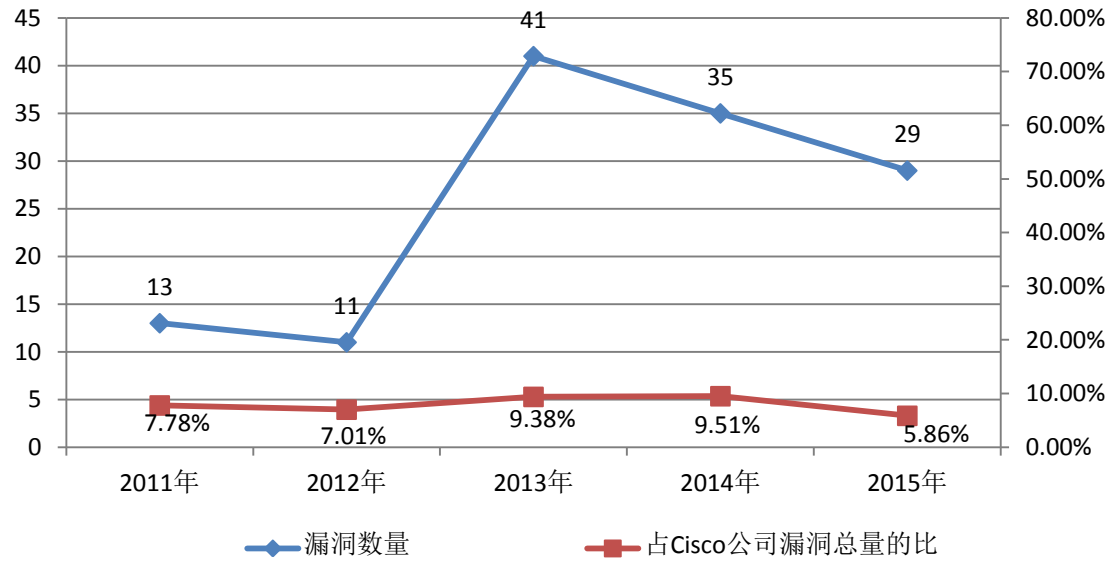

图 30　2011 年至 2015 年 WebEx 产品漏洞数量统计图

3.4.4 NX-OS 产品漏洞数据分析

IOS、XE、XR 和 NX-OS 等都是 Cisco 公司路由器和交换机设备使用的操作系统，其中，除 IOS 外，NX-OS 漏洞数量最多。NX-OS 是一个数据中心级的操作系统，主要运行于 Nexus9000 系列、Nexus7000 系列等交换机设备。根据 2011 年至 2015 年 NX-OS 产品漏洞数量统计图，NX-OS 漏洞数量整体呈上升趋势，2011 年漏洞数量是 2 个，2012 年小幅度增长至 6 个，2013 年出现大幅度上升，达到最高值 32 个，占 Oracle 公司漏洞总量的 19.16%，2014 年下降到 12 个，2015 年出现小幅度回升，增长至 22 个。

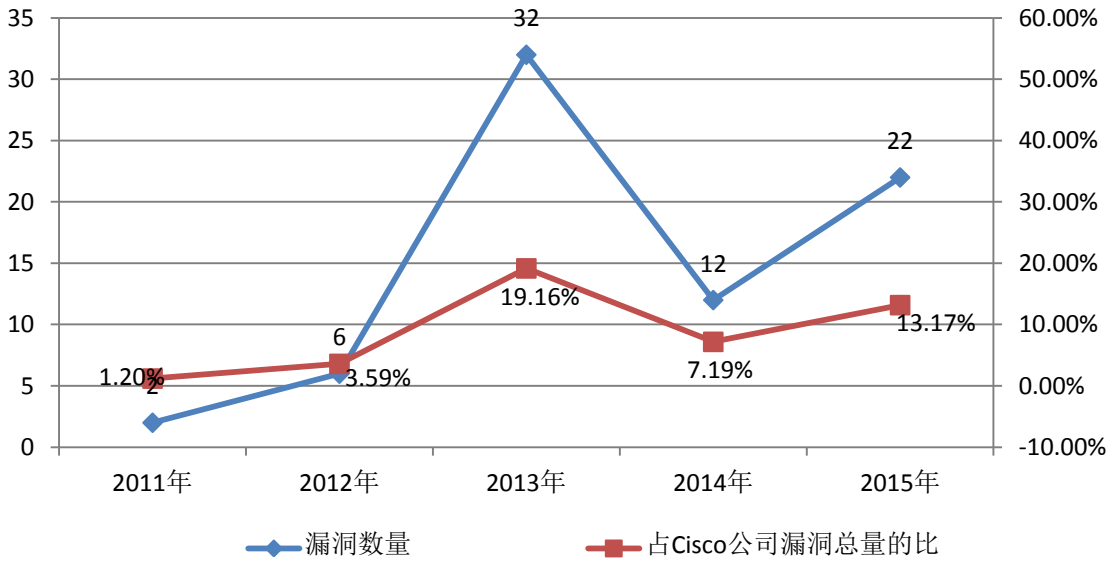

图 31　2011 年至 2015 年 NX-OS 产品漏洞数量统计图

3.4.5 ASA 产品漏洞数据分析

ASA 是 Cisco 公司的一套防火墙设备，该设备还包括 IPS（入侵防御系统）、SSL VPN、IPSec VPN、反垃圾邮件等功能。随着信息安全产业的发展，越来越多的防火墙产品出现在市场，Cisco 公司的 ASA 等防火墙产品市场份额也受到挤压，ASA 市场占有率出现下降趋势。根据 2011 年至 2015 年 ASA 产品漏洞数量统计图，ASA 漏洞数量也呈现出整体下降趋势，并且其漏洞数量占 Cisco 公司漏洞总量的比例也呈现下降趋势。2011 年 ASA 漏洞数量为 31 个，占 Cisco 公司漏洞总量的 18.56%，2012 年下降至 20 个，2013 年又上升至 37 个，2014 年开始逐年下降，2014 年和 2015 年的漏洞数量分别为 26 个和 20 个。

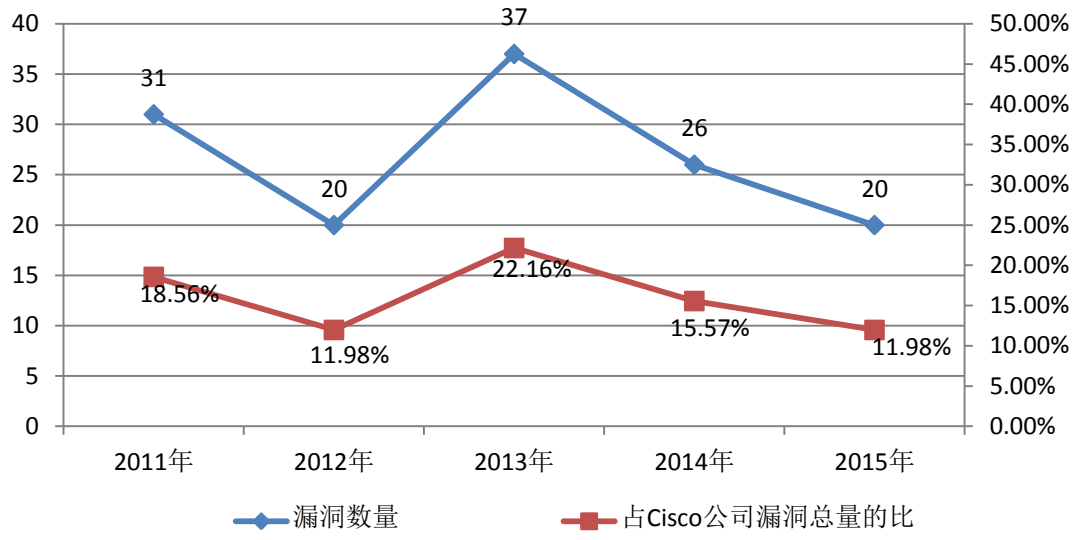

图 32　2011 年至 2015 年 ASA 产品漏洞数量统计图

3.5 Adobe 公司主要产品漏洞数据分析

Adobe 公司是世界著名的数字媒体和在线营销方案的供应商，其产品有 Adobe Creative Suite 图形设计、影像编辑与网络开发套装、Adobe Flash Player 播放器、Adobe Reader 阅读器、Adobe Photoshop 图像处理软件、Adobe Air、ColdFusion 等。

表 13　2015 年 Adobe 公司主要产品新增安全漏洞统计表

序号	产品名称	类型	漏洞数量	所占比例
1	Adobe Flash Player	多媒体播放器	232	68.32%
2	Adobe Air	集成运行时	169	55.28%
3	Adobe Reader	PDF 阅读器	135	28.16%

2015 年该公司主要产品的新增漏洞有 483 个，占 2015 年全年漏洞总数的 6.23%，与 2014 年数量相比增加 346 个，增幅高达 252.55%，且有多种产品增幅超过 200%。其中 Adobe Flash Player 播放器、Adobe Air、Adobe Reader 阅读器等三款主要产品漏洞数量较多，占该公司产品漏洞总数的 90%以上。

3.5.1 Adobe Flash Player 漏洞数据分析

Adobe Flash Player 是一种广泛使用的、专有的多媒体程序播放器。因其使用矢量图形的技术来最小化文件的大小以及创造节省网络带宽和下载时间的文件，成为嵌入网页中的小游戏、动画以及图形用户界面常用的格式。

由 2011 年至 2015 年 Adobe Flash Player 漏洞数量统计图我们可以看出，2011 年至 2014 年该产品漏洞数量处于一个小幅波动的阶段，但是 2015 年该数据有了大幅增加，由 75 个激增至 330 个，增幅高达 340%。但其占主要产品的比例仅从 2014 年的 54.74%增加至 68.32%，主要原因是 Adobe 公司其它几款主要产品在 2015 年的漏洞数量均有大幅度增加。

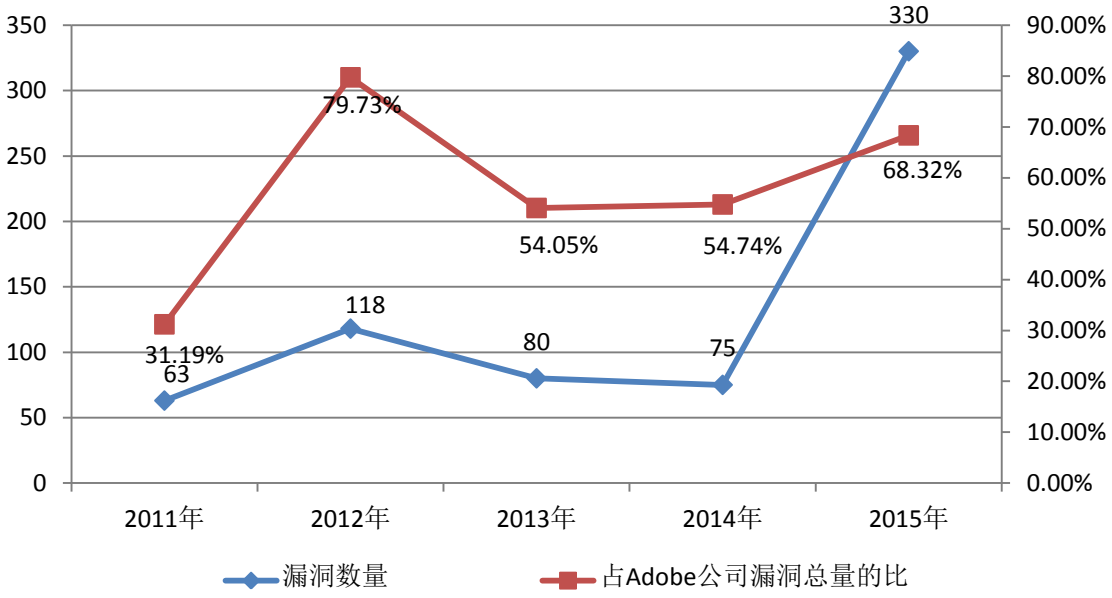

图 33　2011 年至 2015 年 Adobe Flash Player 漏洞数量统计图

3.5.2 Adobe Air 漏洞数据分析

Adobe Air（Adobe 集成运行时）是针对网络与桌面应用的结合所开发出来的技术，用于建立和配置可跨平台或跨操作系统的功能丰富的桌面化互联网应用程序（Rich Internet Applications，RIA）。

和 Adobe Flash Player 类似，Adobe Air 的漏洞数量也在经历了 2011 年至 2014 年的增长及平稳期后，在 2015 年有 317.19%的大幅增长，由 2014 年的 64 个，增加至 2015 年的 267 个。该产品占 Adobe 公司主要产品漏洞数量的比例与其漏洞数量基本成正比。

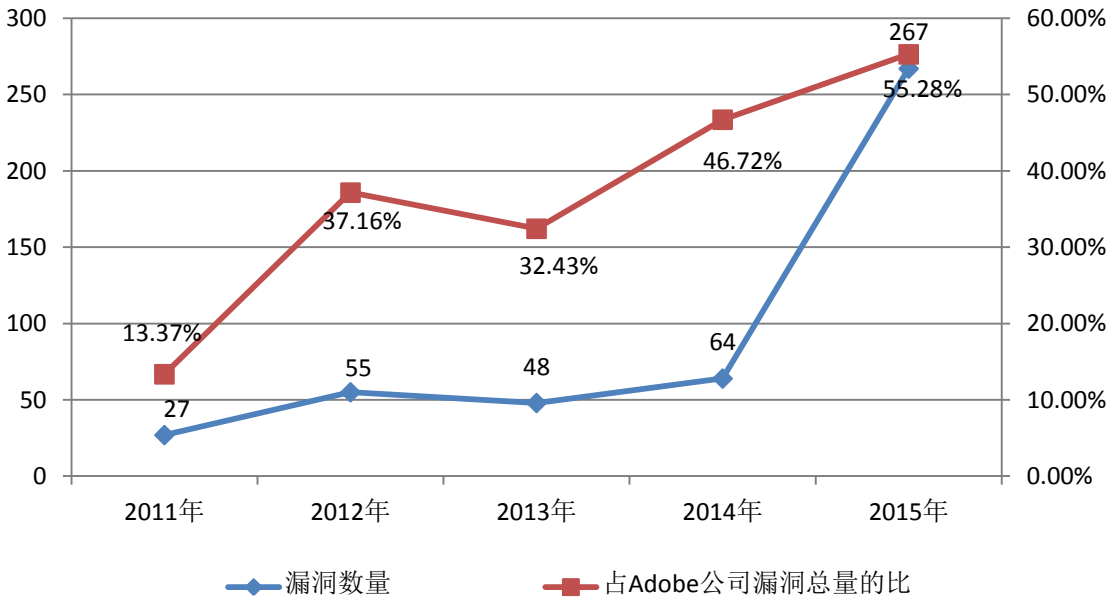

图 34　2011 年至 2015 年 Adobe Air 漏洞数量统计图

3.5.3 Adobe Reader 漏洞数据分析

Adobe Reader 是 Adobe 公司开发的一款 PDF 文件阅读软件，具有非常高的市场占有率和知名度。

由图 36 我们可以看出，该产品漏洞数量一直处于波动的状态，2011 年发现了该产品 60 个漏洞，2012 年这一数据则减少近 50%，减少至 34 个，2013 年则增加了 32 个，增幅达到近 120%，又于 2014 年降至 45 个。与 Adobe 公司其它两款主要产品一样，2015 年该产品漏洞数量也经历了一个激增的过程，大涨 202.22%。

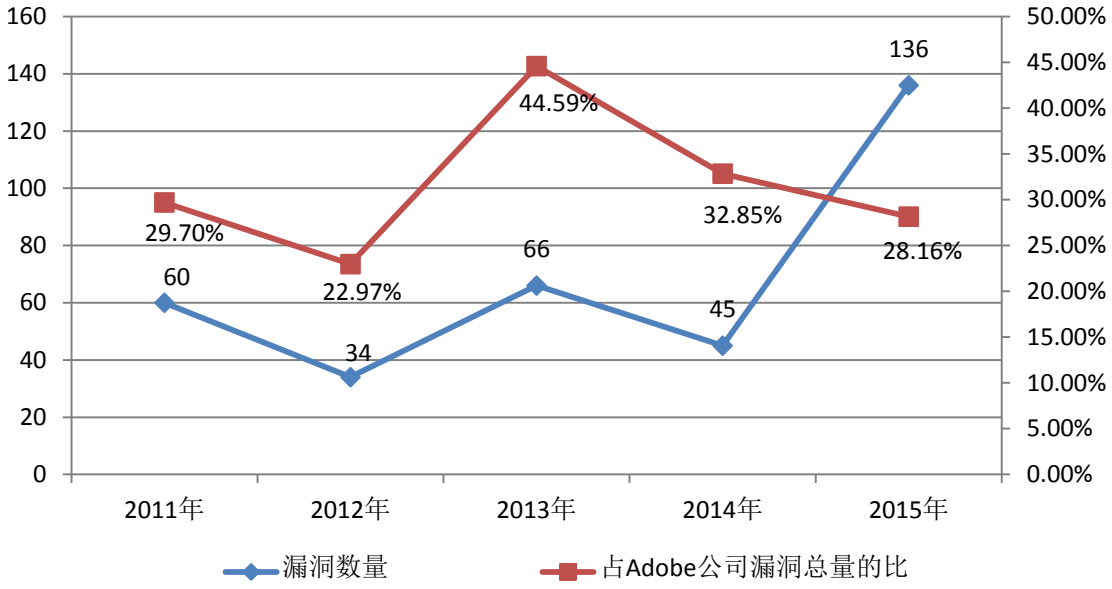

图 35　2011 年至 2015 年 Adobe Reader 漏洞数量统计图

3.6 Google 公司主要产品漏洞数据分析

Google 公司是美国著名科技企业，成立于 1998 年，目前在互联网搜索、云计算、广告技术、移动操作系统等领域，开发并提供了大量知名的基于互联网的产品与服务，并占有较大市场份额，如 Android 移动操作系统、Google Chrome 浏览器、Gmail 电子邮件服务系统、Google glass 可穿戴设备、Google Maps 应用等。2015 年该公司新增漏洞 289 个，占 2015 年全年新增漏洞总数的 3.73%。其中 Google Chrome 浏览器 185 个，Android 移动操作系统 95 个，这两款产品新增漏洞数量占该公司新增漏洞总数 90%以上。

表 14　2015 年 Google 公司主要产品新增安全漏洞统计表

序号	产品名称	类型	漏洞数量	所占比例
1	Google Chrome	浏览器	185	64.01%
2	Android	移动操作系统	95	32.87%

3.6.1 Google Chrome 浏览器漏洞数据分析

Google Chrome，是由 Google 公司开发的浏览器，主要基于开源软件编写。下图是该产品进 5 年来每年漏洞新增数量，从图中可以看出 2011 年至 2014 年，该产品每年的漏洞数量整体呈现下降的态势:由 2011 年的 276 个一路下降至 2014 年的 131 个。2015 年有所反弹，恢复至 2013 年的水品。该产品漏洞占该公司总漏洞数量的比例则基本呈现下降趋势，近两年下降尤为明显。

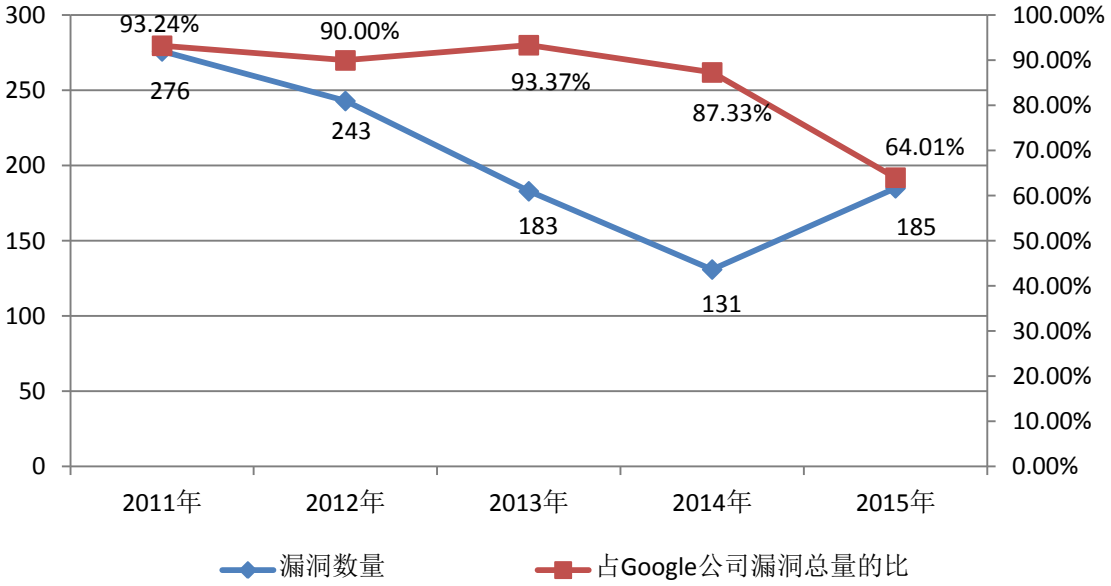

图 36　2011 年至 2015 年 Google Chrome 浏览器漏洞数量统计图

造成这一现象的原因有两点：一是 Google 公司针对 Chrome 增加了一系列安全措施以提高产品的安全性，如禁止了第三方插件在未经用户允许或未向用户提示的情况下自动安装，使得恶意插件入侵用户电脑的情况大大减少；二是近年来全球浏览器市场产品日益增多，Microsoft Internet Explorer、Mozilla Firefox、Apple Safari 和 Opera 等产品正逐步扩大各自的市场占有率，成为了 Chrome 强有力的竞争对手，也分散了漏洞挖掘者对该产品的关注。

3.6.2 Android 移动操作系统漏洞数据分析

Android 移动操作系统是一种基于 Linux 的自由及开放源代码的操作系统，主要使用于移动设备，如智能手机和平板电脑，由 Google 公司和开放手机联盟领导及开发。其作为 Google 公司旗下另外一款主要产品，一直以来都是漏洞挖掘人员关注的重点，尤其是随着移动互联网、移动智能终端的大规模普及，移动支付等服务的广泛应用，移动操作系统安全性更是成为关注热点。

如下图所示，2011 年至 2014 年 Android 移动操作系统漏洞数量处于较为平稳的状态，基本维持在 10 个左右，远小于同期的 iOS 系统的漏洞数据，这与普遍存在的“iOS 系统比 Android 系统安全性更高”的看法并不相同。但在 2015 年，Android 系统漏洞数量有了一个极为明显的增长，增长率高达 630.77%，数量也从 2014 年的 13 个增加至 2015 年的 95 个，但依然远小于 2015 年 iOS 的 375 个。

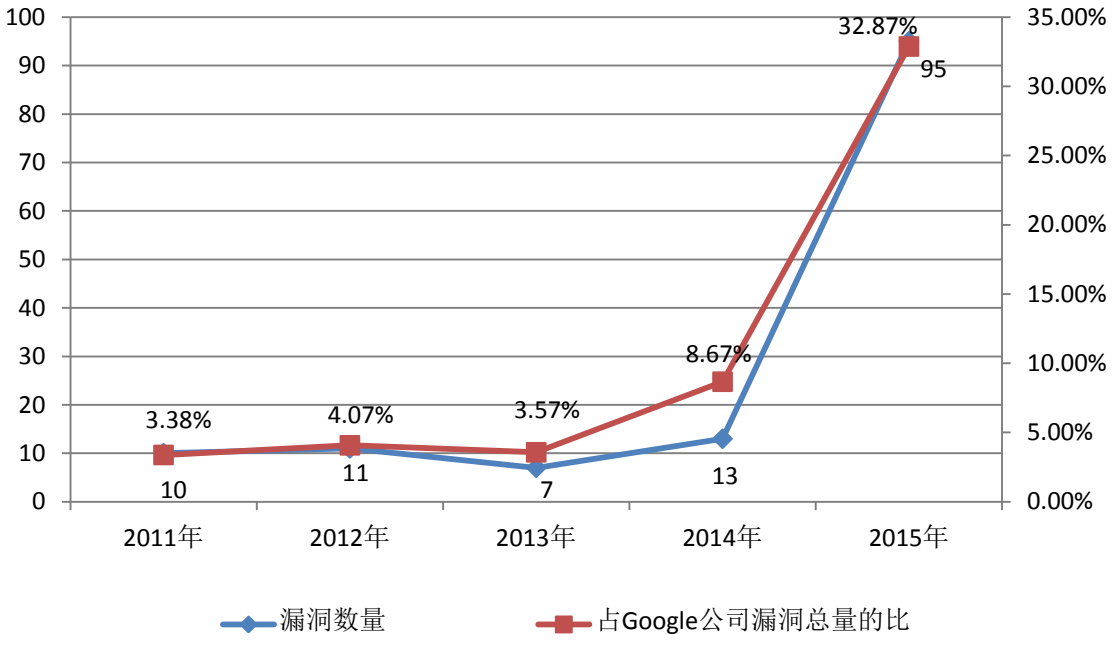

图 37　2011 年至 2015 年 Android 移动操作系统漏洞数据及占比

四、2015 年开源软件重大漏洞情况

开源软件即开放源代码软件，是指软件作者在发布软件时，连同其源代码同时公布的软件。其他开发人员在遵循一定许可协议的情况下，可以按需对软件的源代码进行使用、修改和重新发布。开源软件的类型非常丰富，从操作系统到虚拟云平台、从办公软件到 Web 浏览器、从数据库软件到中间件，开源软件被大量使用。不仅在欧美发达国家中各个行业大量使用开源软件，在我国电信、银行、交通、能源等行业中，重要信息系统和关键基础软件均大量存在基于开源软件进行系统部署和软件研发等情况。

表 15　2015 年开源软件的十大安全漏洞

序号	漏洞名称	CNNVD 编号	发布时间
1	GNU Glibc 基于堆的缓冲区溢出漏洞	CNNVD-201501-658	2015 年 1 月
2	Samba Smbd 代码注入漏洞	CNNVD-201502-363	2015 年 2 月
3	ISC BIND 拒绝服务漏洞	CNNVD-201507-807	2015 年 2 月
4	QEMU Floppy Disk Controller 缓冲区溢出漏洞	CNNVD-201505-207	2015 年 4 月
5	Linux Kernel KCodesNetUSB 模块基于栈的缓冲区溢出漏洞	CNNVD-201505-429	2015 年 5 月
6	Ubuntu Overlayfs 组件提权漏洞	CNNVD-201506-465	2015 年 6 月
7	Android Stagefright 缓冲区溢出漏洞	CNNVD-201507-813、814、815、816	2015 年 7 月
8	Xen 权限许可和访问控制漏洞	CNNVD-201510-789	2015 年 10 月
9	Redis 未授权访问漏洞	CNNVD-201511-230	2015 年 11 月
10	Java 反序列化过程远程命令执行漏洞	CNNVD-201511-241	2015 年 11 月

由于开源软件的应用极为广泛，开源软件的漏洞危害尤其严重，例如：2013 年开源 Web 网络服务器软件 Apache 的 Struts 漏洞，2014 年开源网络加密传输软件 OpenSSL 的“心脏出血”漏洞，2015 年开源 C 语言运行时库 Glibc 的“幽

灵”漏洞、开源虚拟机管理器软件 QEMU 的“毒液”漏洞等。这些漏洞不但在国际上产生了严重的影响，对我国的有关网络信息系统均造成了严重的危害。表 15 为 CNNVD 统计的 2015 年开源软件的十大安全漏洞。

4.1 GNU Glibc 基于堆的缓冲区溢出漏洞

4.1.1 漏洞背景

GNU Glibc（又称 GNU C Library，libc6）是一种按照 LGPL 许可协议发布的开源免费的 C 语言编译程序。Glibc 是 Linux 系统中最底层的 API，除封装 Linux 操作系统所提供的系统服务外，本身也提供了许多一些必要功能服务的实现。

4.1.2 漏洞介绍

GNU Glibc 函数库中__nss_hostname_digits_dots()函数存在缓冲区溢出漏洞，该漏洞是由于 glibc\nss\digits_dots.c 的__nss_hostname_digits_dots 函数未加验证使用 strcpy (hostname, name)，从而导致缓冲区溢出。攻击者可通过应用程序中 gethostbyname()函数发起 DNS 请求，该函数会将主机名称转换为 IP 地址，当提交一个超长又合法的 IP 地址类型的字符串给 gethostbyname()函数，就会造成缓冲区溢出，进而可以利用该漏洞执行任意代码，并获取系统的控制权限。此外，攻击者也可针对 Exim 邮件服务器发起攻击，通过发送特制的邮件，获得远程登录 Linux 系统的 shell 脚本，从而绕过基于 32 位和 64 位系统上的所有现存保护机制（如 ASLR、PIE、NX）。

4.1.3 漏洞影响与危害

该漏洞编号为 CNNVD-201501-658。目前，Debian 7 (wheezy)、 Red Hat Enterprise Linux 6 & 7、CentOS 6&7、Ubuntu 12.04 等大多数 GNU/Linux 发行版本都受此漏洞影响。

4.2 Samba Smbd 代码注入漏洞

4.2.1 漏洞背景

Samba 是在 Linux 和 UNIX 系统上实现 SMB 协议的一个免费软件，由服务器及客户端程序构成。它使用 SMB/CIFS 协议提供一个基于互联网、运行在 TCP/IP 协议之上的网络文件和打印共享服务，还可以集成动态目录环境，使得服务器主机作为域控制器或作为一个域成员。其中，Smbd 是 Samba 的服务端进程，通过 SMB/CIFS 协议为客户端（如 Windows 95、98、ME，Windows NT 和 Windows 2000 等）提供文件共享和打印服务。2015 年 2 月 23 日，Red Hat 产品安全团队披露该漏洞。

4.2.2 漏洞介绍

Samba Smbd 代码注入漏洞是由于守护进程 Smbd 处理 Netlogon 数据包的功能存在缺陷，通过使用一个 IPC 空会话调用处理 NetLogon 服务相关的 RPC API 接口 ServerPasswordSet 函数，可导致一个未初始化指针传递给 TALLOC_FREE() 函数，从而触发该漏洞。攻击者可借助特制的 Netlogon 数据包利用该漏洞执行执行任意代码。该漏洞触发并不需要通过 Samba 服务器的账号认证，而 Smbd 服务端通常以 root 权限运行，如果漏洞能够被用来实现任意代码执行，则攻击者可以远程获取系统 root 权限，危害极其严重。

4.2.3 漏洞影响与危害

该漏洞编号为 CNNVD-201502-363。此漏洞几乎影响所有版本，即从 Samba 3.5.x 版本和 3.6.25 之前的 3.6.x 版本，4.0.25 之前的 4.0.x 版本，4.1.17 之前的 4.1.x 版本，4.2.0rc5 之前的 4.2.x 版本。由于 Samba 组件广泛应用于 Linux 和 UNIX 系统，致使主流 GNU/Linux 发行版也都受到严重影响。

4.3 ISC BIND 拒绝服务漏洞

4.3.1 漏洞背景

ISC BIND 是美国 Internet Systems Consortium（ISC）公司所维护的一套实现了 DNS 协议的开源软件。

4.3.2 漏洞介绍

ISC BIND 9 TKEY 存在拒绝服务漏洞，该漏洞是由于 TKEY 查询错误导致 BIND 服务器发生 REQUIRE 断言失败并停止服务，远程攻击者可借助 TKEY 查询利用该漏洞对 BIND 所在服务器进行攻击，耗尽 CPU 资源及网络资源，直至该 DNS 服务器崩溃。

4.3.3 漏洞影响与危害

该漏洞编号为 CNNVD-201507-807。该漏洞影响 BIND 9 所有版本（包括 BIND 9.1.0 版本至 BIND 9.9.7-P1，BIND 9.10.0 至 BIND 9.10.2-P2 版本），及互联网上对应版本的递归服务器和权威服务器。

据统计，我国约有 42 万余台 DNS 服务器，其中使用 ISC BIND 服务的服务器有 29,913 台，占总量 7.1%。该漏洞对我国基础网络稳定有较大的威胁，一旦遭受网络攻击将引发 DNS 服务异常，从而会导致大范围网络中断。

4.4 QEMU Floppy Disk Controller 缓冲区溢出漏洞

4.4.1 漏洞背景

QEMU 是由法国程序员 Fabrice Bellard 所研发的一套开源模拟处理器软件。该软件广泛用于各大 GNU/Linux 发行版（包括 Debian, Gentoo, SUSE, RedHat,CentOS 等）。QEMU 提供的仿真外设包括硬件 Video Graphics Array (VGA) 仿真器、PS/2 鼠标和键盘、集成开发环境（IDE）硬盘和 CD-ROM 接口，以及软盘仿真等。

4.4.2 漏洞介绍

该漏洞存在于 QEMU 虚拟软盘驱动器（FDC）模块，具体位于 QEMU 的虚拟软驱控制器的模拟代码中，而 FDC 代码应用于众多虚拟化平台和设备中，尤其是 Xen、KVM 以及本地 QEMU 客户端。虚拟机操作系统通过 FDC（该代码广泛应用于虚拟化平台和设备中）的输入输出端口发送搜索、读取、写入、格式化等指令与 FDC 进行通信。QEMU 的虚拟 FDC 通常会根据一定的算法为指令预留和跟踪存储资源，执行指令并重置缓冲区。攻击者可以从受感染虚拟机中摆脱访客身份限制，通过客户系统发送命令和构造的参数数据到 FDC 软盘控制器，以此导致数据缓冲区溢出，从虚拟机系统完成“逃逸”，达到在宿主机监控程序进程环境下执行任意代码的攻击目的。同时，攻击者可以访问宿主机系统以及主机上运行的所有虚拟机，并能够提升重要的访问权限，进而影响到宿主机所在本地和相邻网络。

4.4.3 漏洞影响与危害

该漏洞编号为 CNNVD-201505-207。该漏洞影响 Xen 4.5.x 及之前版本和 KVM 2.3.0 及之前版本。目前，由于大部分机构和用户都依靠受影响的虚拟化平台来分配共享的计算资源、连接、存储、安全以及隐私服务，为此该漏洞可导致到成千上万的企业知识产权的访问权限和敏感数据得到公开，甚至内网被渗透。同时数以百万计的终端用户个人身份信息遭到泄露。具体影响情况为：（1）虚拟机宕机，影响业务；（2）系统资源被强制占用，宿主机及所有虚拟机拒绝服务；（3）攻击者在宿主机中执行任意代码。

4.5 Linux Kernel 基于栈的缓冲区溢出漏洞

4.5.1 漏洞背景

Linux Kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。KCodesNetUSB 是其中的一个用来共享家庭用户网络的 USB 设备模块。该漏洞由奥地利安全公司 SEC Consult 的研究员 Stefan Viehbock 于 2015 年 5 月披露，由于涉及到的厂商众多，影响数以百万计的路由和嵌入式设备，受到国内外的广泛关注。

4.5.2 漏洞介绍

Linux Kernel KCodesNetUSB 模块中的‘run_init_sbus’函数存在基于栈的缓冲区溢出漏洞。远程攻击者可通过在 TCP 20005 端口的会话中提供超长的计算机名称并利用该漏洞执行任意代码。如果客户端发送的计算机名长度大于 64 字符，会让含 NetUSB 模块的设备出现溢出，从而造成内存破坏。因为服务端

缺乏足够的验证，过长的计算机名可能会被黑客利用来进行内核溢出攻击，最后可能会演变成远程代码攻击或者 DoS 攻击。

4.5.3 漏洞影响与危害

该漏洞编号为 CNNVD-201505-429。Linux kenel Kcodes NetUSB 模块在多款 NETGEAR 产品和 TP-Link 产品中使用，攻击者通过利用该漏洞，可以在内核层面远程执行恶意代码，控制路由等网络设备，从而可对网络设备发起进一步的攻击。

4.6 Ubuntu Overlayfs 组件提权漏洞

4.6.1 漏洞背景

Ubuntu 是英国科能（Canonical）公司和 Ubuntu 基金会共同开发的一套以桌面应用为主的 GNU/Linux 操作系统，Overlayfs 是其中的一个文件系统服务。

4.6.2 漏洞介绍

Ubuntu 中的 Overlayfs 组件存在本地提权漏洞，该漏洞是由于 Overlayfs 文件系统在上层文件系统目录中创建新文件时没有正确检查文件权限。本地攻击者可利用该漏洞获取目标系统的管理员权限，执行任意操作，在敏感系统目录中创建新文件或读取敏感文件内容。Overlayfs 只检查了被修改文件的属主是否有权限在上层文件系统目录写入，导致当从底层文件系统目录中拷贝一个文件到上层文件系统目录时，文件属性也随同拷贝过去。如果 Linux 内核设置了 CONFIG_USER_NS=y 和 FS_USERNS_MOUNT 标志，将允许一个普通用户在

低权限用户命名空间中嵌入一个 Overlayfs 文件系统。本地攻击者可利用该漏洞获取系统的管理员权限，从而完全控制受影响计算机。

4.6.3 漏洞影响与危害

该漏洞编号为 CNNVD-201506-465。目前，针对该漏洞的利用代码已经公开，恶意攻击者不需要较深的技术水平就能对存在漏洞的对象发起攻击，尽管厂商已发布修复补丁，但仍有不少主机受到攻击和破坏。

4.7 Android Stagefright 缓冲区溢出漏洞

4.7.1 漏洞背景

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统，主要应用于移动设备。其中，Stagefright 是一款安卓内置的媒体播放工具。该漏洞由 Zimperium 公司安全研究人员舒亚·德雷克(JoshuaDrake) 于 2015 年 7 月披露。

4.7.2 漏洞介绍

Android 处理媒体格式的 libstagefright 代码库中 MPEG4Extractor.cpp 文件存在四处缓冲区溢出漏洞，攻击者可借助特制数据利用该漏洞造成拒绝服务（整数溢出和内存损坏），执行恶意代码控制设备，进而窃取各类数据，包括信用卡或个人信息。安全公司 Zimperium 已公开了攻击代码，该攻击代码能生成一个利用漏洞的 MP4 媒体文件，攻击者可以在麦克风的听觉范围内监听声音，以及利用摄像头拍摄照片。

4.7.3 漏洞影响与危害

上述四个漏洞编号分别为 CNNVD-201507-813、CNNVD-201507-814、CNNVD-201507-815、CNNVD-201507-816。漏洞影响 Android 5.1 及之前版本，涉及 95%的 Android 设备。虽然 Google 已经将补丁应用到谷歌内部的 Android 代码库中，由于 Android 更新较慢，Android 补丁到达终端用户手中往往需要几个月时间，所以仍有大量 Android 设备受到影响。

4. 8 Xen 权限许可和访问控制漏洞

4.8.1 漏洞背景

Xen 是由剑桥大学开发的一款开源虚拟机监视系统，该产品能够使不同或不兼容的操作系统运行在同一台计算机上，并支持在运行时进行迁移，保证正常运行并且避免宕机。目前，该系统广泛应用于亚马逊 EC2、阿里云 ECS、IBM SoftLayer、Linode 及 Rackspace Cloud 等主流厂商的云计算服务。2015 年 10 月 29 日，Xen 官方在公告中公布“虚拟机系统软件 Xen 权限许可和访问控制漏洞”，该漏洞已存在长达 7 年之久。

4.8.2 漏洞介绍

Xen 系统的 arch/x86/mm.c 文件中的‘mod_l2_entry’函数存在权限许可和访问控制漏洞，该漏洞源于程序没有正确验证二级页表的条目。本地攻击者可借助特制的 superpage 映射来利用该漏洞获取权限，最终绕过软硬件上的所有安全机制的限制，以及 Xen Hypervisor 上下文环境和 Dom0 上下文环境执行任意代码。攻击者可利用该漏洞提升普通用户权限，进而控制整个虚拟机系统，造成用

户数据泄露或丢失，甚至可从外网直接进入虚拟化环境内网，对云计算厂商的内网环境进行进一步的入侵和渗透。

4.8.3 漏洞影响与危害

该漏洞编号为 CNNVD-201510-789。该漏洞主要影响 Xen 平台 3.4 版本至 4.6.x 版本的 PV 模式下运行的虚拟机。由于 Xen 项目是实现云计算虚拟化的基础，承载着全球大部分的公有云计算业务，此次漏洞已导致全球大部分的云服务提供商短暂停机，其中亚马逊和云计算厂商 Rackspace 的服务器受漏洞影响而需重启。

4.9 Redis 未授权访问漏洞

4.9.1 漏洞背景

Redis 是美国 Redis Labs 公司研发的一套开源数据库，该数据库使用 ANSI C 编写，支持网络操作，可基于内存亦可持久化地进行日志型、键值存储，并提供多种语言的 API。2015 年 11 月 4 日，Redis 的作者 Salvatore Sanfilippo 针对早前的“Redis 未授权访问漏洞”公开了其漏洞利用方法，即：Redis 可通过写入 SSH Key 进而控制服务器，大量黑客使用该漏洞利用工具，对 Redis 访问接口进行恶意攻击，从而引发全球性安全事件。

4.9.2 漏洞介绍

Redis 未授权访问安全漏洞是由于默认情况下 Redis 开启 6379 端口，若未开启认证且无任何防护策略，任意用户可在未授权的情况下访问 Redis 并读取相关数据。远程攻击者可利用该漏洞直接取得目标服务器管理权，进而造成当前

Redis 版本、内存运行状态、服务端个数等敏感信息以及数据库数据泄露，同时可远程执行任意代码。

4.9.3 漏洞影响与危害

该漏洞编号为 CNNVD-201511-230。据悉，目前全球互联网上可直接访问的 Redis 服务有 97700 个，其中未经验证可直接利用该服务的目标主机有近 5 万个，已遭受漏洞攻击主机占比 65%（3.1 万个）。我国境内存在该类目标主机共计 1.6 万多个，已遭受漏洞攻击主机占比 67.5%（1.1 万个）。由该漏洞引发的大规模安全攻击事件中，我国杭州、北京、广州等多地上百家单位受到敏感信息泄露等严重影响，涉及政府网站、互联网金融公司、教育系统等多个行业和领域。

4. 10 Java 反序列化过程远程命令执行漏洞

4.10.1 漏洞背景

Apache Commons 是一种集合所有可用 Java 组件的 Apache 项目，其包含多个开源工具的工具集，可解决编程问题并减少重复劳动，主要应用于 Java 技术平台，WebLogic、IBM WebSphere、JBoss、Jenkins 和 OpenNMS 等。《Marshalling Pickles》报告中曾提出 Java 反序列化漏洞可利用 Apache Commons Collections 实现任意代码执行的观点，并提供相应的 Payload 生成工具。2015 年 11 月 6 日，针对最新版的 WebLogic、WebSphere、JBoss、Jenkins、OpenNMS 等主流 Java 应用再次提出该漏洞利用方法。

4.10.2 漏洞介绍

Apache Commons Components Invoker Transformer 反序列化任意代码执行漏洞是由于 Apache Commons Collections 组件的 Deserialize 功能存在的设计漏洞，Commons Collections 组件中对于集合的操作存在可以进行反射调用的方法，且该方法在相关对象反序列化时并未进行任何校验，远程攻击者利用漏洞可发送特殊的数据给应用程序或给使用包含 Java “InvokerTransFormer.class” 序列化数据的应用服务器，在目标服务器当前权限环境下执行任意代码。

4.10.3 漏洞影响与危害

该漏洞编号为 CNNVD-201511-241。Apache Commons 工具广泛应用于 Java 技术平台，WebLogic、IBM WebSphere、JBoss、Jenkins 和 OpenNMS 等应用都大量调用了 Commons 工具集，所以攻击者可利用该漏洞对这些应用发起远程攻击。

五、2015 年信息安全漏洞管控发展情况

5.1 美将零日漏洞技术纳入出口管控

目前，网络空间已经成为继陆、海、空、天之后的第五空间，成为新形势下维护国家安全的重要领域之一，网络空间的安全已成为国家安全的战略高地。为保障国家网络安全，必然要全面推进网络空间法治化，加强网络空间和信息化领域的法治建设。在维护网络安全的各种手段中，加快网络安全立法是根本保障。美国等国家高度重视网络安全立法，一方面加快出台网络安全基本法，另一方面强化政府信息安全、信息监控与内容安全、数据保护、关键基础设施保护等多方面立法，为网络安全保护各项措施的具体实施提供法律依据。为了加强政府对信息安全漏洞的监管，美国于 2015 年相继出台了《瓦森纳协定》（Wassenaar Arrangement）的补充协定和《网络空间安全信息共享法》，作为针对未公开漏洞的出口限制禁令，以及企业间共享网络安全信息的法律保障。

2015 年 5 月，美国商务部工业与安全局公布了一项“把限制黑客技术放入全球武器贸易条约”的计划，并提交了新的出口限制禁令，作为由美、英、法、意等国签署的现行《瓦森纳协定》的补充。

《瓦森纳协定》又称瓦森纳安排机制，全称为《关于常规武器和两用物品及技术出口控制的瓦森纳安排》（The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Good and Technologies），是一种建立在自愿基础上的集团性出口控制机制，根本目的在于通过成员国间的信息通报制度，提高常规武器和双用途物品及技术转让的透明度，以达到对常规武器和双用途物品及相关技术转让的监督和控制。该协定的签署主要基于 1995 年 9 月在荷兰瓦森纳召开的一次高官会议，参与者包括美国、英国、法国、意大利等“巴黎统筹委员会”（对社会主义国家实行禁运和贸易限制的国际组织，于 1994

年正式宣告解散，其下建设有中国委员会，是对中国实行禁运的执行机构）17 国在内的 28 个国家，会议决定加快建立常规武器和双用途物资及技术出口控制机制，弥补现行大规模杀伤性武器及其运载工作控制机制的不足。1996 年 7 月，美国以此为基础，在奥地利维也纳联合澳大利亚、比利时、西班牙等西方国家为主的 33 个国家签署了《瓦森纳协定》，并决定从 1996 年 11 月 1 日起实施新的控制清单和信息交换规则。《瓦森纳协定》包含两份控制清单：一份是军民两用商品和技术清单，涵盖了先进材料、材料处理、电子器件、计算机、电信与信息安全、传感与激光、导航与航空电子仪器、船舶与海事设备、推进系统等 9 大类；另一份是军品清单，涵盖了各类武器弹药、设备及作战平台等共 22 类。成员国对控制清单上物项的出口实行国家控制，即由各国政府自行决定是否允许或拒绝转让某一物品，并在自愿基础上向其他成员国通报有关信息，协调控制出口政策。信息交换仅限于向非成员国的出口，成员国间的贸易无需通报。大多数发展中国家都受到该协定的限制，中国不是该协定的成员国，也在被禁运国家之列。

2015 年这份新的出口限制禁令的出台，将未公开的软件漏洞（即零日漏洞）视为潜在的武器进行限制和监管。该禁令规定，在未经特别许可的情况下，禁止在美国、英国、加拿大、澳大利亚以及新西兰等国之外销售零日漏洞及其相关产品。通过“出口限制禁令”，美国政府限制了零日漏洞及其相关产品流出美国，但是依据现行的《网络空间安全国家战略》，美国政府可通过美国国家漏洞库（NVD）面向全球收集漏洞，Microsoft、Cisco、Apple、Adobe 等全球主要软硬件厂商的产品漏洞都在美国国家漏洞库的掌握之中。一直以来，美国在信息安全技术方面遥遥领先，而通过“出口限制禁令”的“堵”和 NVD 对全球漏洞的“收”，美国政府又有效增强了对全球漏洞的掌控，使美国在网络空间的战略优势继续扩大。

5.2 漏洞相关标准体系更加完善

漏洞标准是关于漏洞命名、评级、检测、管理的一系列规则和规范。漏洞的标准化是确保信息安全系统以及信息安全产品在设计、研发、生产、建设、使用和测评中解决其一致性、可靠性、可控性、先进性和符合性的技术规范、技术依据。信息安全漏洞标准是信息安全保障体系的重要组成部分，是对漏洞进行有效管理的重要手段。

5.2.1 常用漏洞标准

在漏洞相关标准的制定方面，美国的 NIST（National Institute of Standards and Technology，美国国家标准与技术研究院）、FIRST（Forum of Incident Response and Security Teams，事件响应与安全团队论坛）和 MITRE（美国麦特公司）等机构、组织和公司，相继推出了 CVE、CCE、CVSS 等一系列有影响力的标准。经过多年的发展，部分标准已经得到了广泛的认可，被很多企业和组织机构所采用，成为了事实上的工业标准。这些标准有 CVE、CVSS、CWE、CWSS、CCE、CPE、OVAL 和 XCCDF，简介如下：

1、 CVE（Common Vulnerability & Exposures，通用漏洞披露）是 MITRE 公司制定的一个面向公开披露的信息安全漏洞的通用命名标准。CVE 通用命名可以使不同的漏洞库和安全产品之间共享信息，并为安全工具的检测结果提供评估基准。

2、 CVSS（Common Vulnerability Scoring System，通用漏洞评分系统）是 FIRST 组织发布的一个用于评估信息安全漏洞严重程度的度量标准。

3、 CWE（Common Weakness Enumeration，通用缺陷枚举）是 MITRE 公司制定的一套软件缺陷的枚举清单与分类规范，其目的是为软件架构、设计和代码中的安全缺陷提供一个通用的描述语言。

4、 CWSS（Common Weakness Scoring System，通用缺陷评分系统）是 MITRE 公司提供的一个对软件缺陷进行风险评价的通用框架。

5、 CCE（Common Configuration Enumeration，通用配置枚举）列表为每个安全相关的系统配置问题提供一个通用的、唯一的标识符，利用 CCE 标识符可以在不同信息源和安全工具间共享系统配置数据。CCE 最初由 MITRE 公司开发，现在已移交给 NIST 进行管理和维护。

6、 CPE（Common Platform Enumeration，通用平台枚举）是一个对应用程序、操作系统以及硬件设备进行描述和标识的标准化方案，它提供了一个标准的机器可读的格式，利用这个格式可以对 IT 产品和平台进行编码。与 CCE 一样，CPE 最初也由 MITRE 公司开发的，现在也已移交给了 NIST 进行管理和维护。

7、 OVAL（Open Vulnerability and Assessment Language，开放漏洞与评估语言）是一个对计算机系统的安全状态进行评估和报告的国际化标准化语言。OVAL 是一个由信息安全社区开发的语言，一直由 MITRE 公司进行维护和管理，近期，MITRE 将其移交给了非盈利组织 CIS（Center for Internet Security，因特网安全中心）。

8、 XCCDF（eXtensible Configuration Checklist Description Format，可扩展的配置清单描述格式）是由 NIST 制定的一个编写安全检查清单、基准和相关类型文档的规范语言。一个 XCCDF 文档表示一个结构化的安全配置规则集。

在这八个常用的标准中，CVE、CVSS、CWE、CWSS、OVAL 和 CPE 六个标准更是被国际电信联盟（International Telecommuniction Union，简称 ITU）纳入到了其 X 系列（数据网、开发系统通信和安全性）建议书中，成为了 ITU

向全世界范围推荐的网络安全信息交换国际标准。下表中给出了这些标准对应的 ITU-T 建议书编号和批准时间。

表 16　漏洞标准及 ITU-T 建议书编号

漏洞标准	ITU-T 建议书编号	首次纳入时间	最新版批准时间
CVE	ITU-T X.1520	2011-04	2014-01
CVSS	ITU-T X.1521	2011-04	2011-04
CWE	ITU-T X.1524	2012-03	2012-03
CWSS	ITU-T X.1525	2015-04	2015-04
OVAL	ITU-T X.1526	2013-04	2014-01
CPE	ITU-T X.1528	2012-09	2012-09

5.2.2 漏洞标准体系

尽管这些标准已经得到了广泛的应用，并且很多已经成为了国际标准，然而，它们仍然是一些孤立的标准，没有形成一个完整的标准体系。为了将这些独立的标准进行整合，使其发挥更大的作用，NIST 联合多个机构共同提出了安全内容自动化协议（The Security Content Automation Protocol，简称 SCAP）。SCAP 由多个可相互交互的信息安全标准组成，其标准化、自动化的思想对信息安全行业产生了深远的影响。目前，以 SCAP 为核心形成了当前国际上比较成熟的一套信息安全漏洞评估标准体系。

当前实际使用的 SCAP 版本是 1.0 版，这个版本包含 6 个 SCAP 元素，分别是：XCCDF、OVAL、CVE、CCE、CPE 和 CVSS。这些元素可以分为三种类型：1）语言类，用来描述评估内容和评估方法的标准，包括了 XCCDF 和 OVAL；2）枚举类，描述对评估对象或配置项命名格式，并提供遵循这些命名的库，包

括了 CVE、CCE、CPE；3）度量类，提供了对评估结果进行量化评分的度量方法，对应的元素是 CVSS。

信息安全标准体系仍在继续发展和完善，2015 年，SCAP 的最新版本已经发展到了 1.2 版，在这一版中除了对部分已有标准进行更新外，还引入了新的标准规范。

SCAP 1.2 版中引入的新的标准有 CCSS、ARF、AI、TMSAD 和 OCIL，它们的简介如下：

1、 CCSS（ Common Configuration Scoring System，通用配置评分系统），是一个用于度量系统配置缺陷严重程度的度量标准。

2、 ARF（Asset Reporting Format，资产报告格式）是一个数据模型，用来表达关于资产、资产和报告之间关系信息的传输格式。

3、 AI（Asset Identification，资产识别）提供了基于已知标识符和/或已知的信息资产进行唯一地资产标识的规范。

4、 TMSAD（Trust Model for Security Automation Data，安全自动化数据的信任模型）描述了一个共同的信任模型，该模型可以应用到安全自动化领域。

5、 OCIL（Open Checklist Interactive Language，开放清单交互式语言）定义了一个框架，这个框架用于表达软件使用的调查问卷，目的是为了收集先前工作存储的信息或是为了收集来自于人的信息。

在 1.2 版中，SCAP 还对部分标准进行了更新，这些更新主要包含如下内容：

1、 CVE -ID 语法格式出现新的变化。为了应对安全漏洞数量迅速增长的情况，CVE 编辑委员会和 MITRE 公司决定对 CVE-ID 的编码格式进行修改，通过采用可变长的格式以使其每年能够收录更多的漏洞。

2、 CPE 发展到了 2.3 版。CPE 2.3 中新的命名格式与 URI 语法格式有所不同，通过引入 WFN（well-formed CPE name，结构良好的 CPE 命名）结构并定义了使用该结构构建机器可读的编码格式的方案，为未来机器间交换产品名称描述的方式做好了铺垫。

3、 CCE 为每一个通用系统配置问题提供一个唯一的标识符，主要用于处理错误配置问题。CCE 列表为安全相关的系统配置问题提供唯一的标识符，CCE 的最新发布版是 CCE 5.20130214，与上一版相比（CCE 5.20120314），增加了 948 个新的条目，10 个新的平台组。

4、 CVSS 是用于评估系统安全漏洞严重程度的标准。CVSS 2.0 版本没有明确说明在哪个攻击点上 CVSS 值应该被计算，这导致得分指标之间的差异受影响。CVSS 新发布的 3.0 版本对此作出了明确的规定，CVSS 得分是在当第一次攻击对机密性、完整性和可用性造成影响时进行计算的。

5.3 漏洞交易的市场化成为常态

目前的漏洞管理方式实际上是对漏洞信息的一种聚集，各级机构试图利用自身在政策、技术、经济方面的优势对所搜集的漏洞资源进行垄断。但是漏洞管理机构不可能掌握所有的漏洞信息，也不可能网罗所有的漏洞挖掘者。隐藏在民间的技术顶尖的漏洞挖掘人员往往通过地下方式进行漏洞交易，获取非常可观的利润，而这种交易的市场化已成为常态。

2015 年初，网络上出现了一个名为“真正交易”（The Real Deal）的黑市，它的主要业务是向黑客兜售零日漏洞利用工具。不同于目前市面上的其它网站只售卖基本的低级黑客工具以及泄露的财务信息，“真正交易”使用 Tor 匿名技术加密连接，交易则使用比特币，以隐藏买家、卖家、管理员的身份，从而吸引高

端黑客在售卖零日漏洞、源代码，甚至提供黑客雇佣服务。

2015 年 11 月，零日漏洞中间商 Zerodium 公司公布了一份不同类型“数字化入侵技术与软件目标”的漏洞报价的清单，这份清单列出了面向数十种不同应用程序及操作系统的具体黑客攻击方法，每一项都提供极为详细的实现方式以及对应的漏洞报价。原图如下：

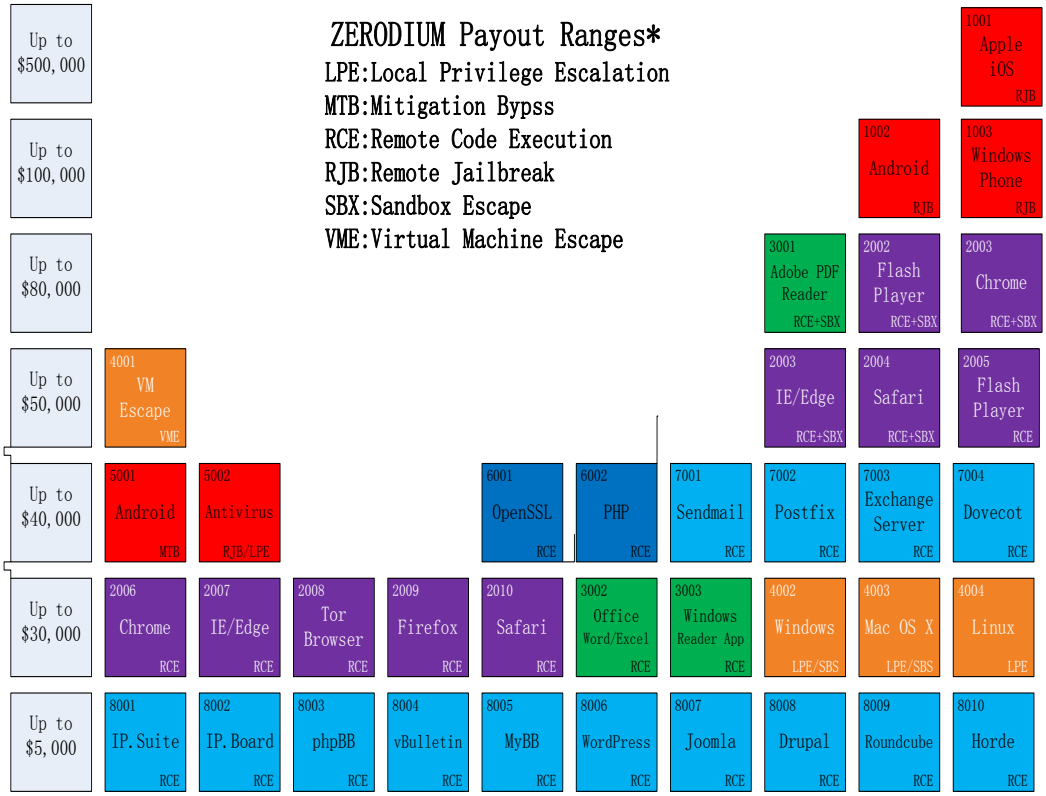

图 38　Zerodium 数字化入侵技术与软件目标漏洞报价

清单中包括本地特权逃逸（LPE）、缓解旁路（MTB）、远程代码执行（RCE）、远程越狱（RJB）、沙箱逃逸（SBE）、虚拟机逃逸（VME）六种漏洞攻击方式，交易价格从 5 千到 50 万美元，其中 Apple iOS、Android、Adobe 漏洞价格最高。而在 2015 年 9 月，Zerodium 公司发起了一个 BUG 赏金活动，在截至 10 月 31 日之前提交的关于 iOS 9 前三个 0-Day 漏洞每个漏洞都可获得最高 100 万美元的奖金。

随着漏洞交易市场完善，明码标价，地下黑市中流通的高危漏洞大量增加，

其所造成的危害也日益严重。

5.4 国内厂商纷纷成立安全应急响应部门

随着信息安全漏洞的数量、影响及危害日益增加，国内许多厂商对自身产品的安全性也愈发重视，纷纷成立安全应急响应部门，以便第一时间收录和处置旗下相关产品及业务的安全漏洞和威胁信息，消除安全隐患。截至 2015 年底，国内已有近 30 余家厂商建立了相应部门（具体情况见表 17）。

5.4.1 应急响应部门发展情况

知名互联网公司率先建立应急响应部门。2012 年 5 月，腾讯公司成立了“腾讯安全应急响应中心（TSRC）”，这也是国内第一家此类机构。随后，百度公司和阿里巴巴集团也分别于 2013 年 6 月、2013 年 10 月宣布建立了各自的安全应急响应中心。360 安全应急响应中心于 2013 年 12 正式公布了《漏洞报告与处理流程》，至此，“BAT3”互联网巨头完成了对安全应急响应部门的初期建立。与此同时，网易、新浪、金山、小米等互联网公司也纷纷加入应急响应建设的队伍中，收录各自产品的漏洞。

电子商务、保险金融公司积极建设应急响应部门。由于自身业务特性，为了避免巨大的经济和信誉损失，电商、保险金融公司也纷纷建立安全应急响应部门。建设安全应急相应部门的投入与漏洞可能造成的损失相比，则显得十分划算。于是从 2013 年开始，几乎所有的知名电商如京东、苏宁、1 号店、携程、去哪儿等公司的应急响应部门如雨后春笋般涌现，2015 年则有两家电商公司成立了应急响应部门，分别是滴滴出行和同程旅游。其中同程旅游在“同程安全应急响应中心”网站上宣布成为“国内第一家公开自家漏洞供白帽子们学习”的公司。在保险金融公司方面，平安集团成立了国内第一家保险金融类应急响应部门：平安

安全应急响应中心；阿里巴巴集团则在已建立集团应急响应中心的情况下，为支付宝、支付宝钱包、余额宝、招财宝、蚂蚁小贷和网商银行等蚂蚁金融服务集团的业务单独建立了“蚂蚁金服安全应急响应中心”。

国内传统硬件、软件服务厂商也开始关注自身漏洞的收集。2015 年 4 月，联想安全应急响应中心漏洞提交平台正式上线，升级漏洞奖励计划，对符合条件的漏洞提交人员进行积分以及礼品奖励；2015 年 7 月，海康威视公司“萤石安全应急响应中心”正式发布漏洞奖励计划。华为集团通过“华为产品安全事件响应团队（PSIRT）”统一接收、处理和公开披露华为产品和解决方案相关的安全漏洞，另一家通信解决方案提供商中兴通讯则公布了“白帽子奖励计划”，用以奖励发现其 IT 系统的安全漏洞或风险，以及泄密或窃密信息。

5.4.2 运行及奖励机制

目前，绝大多数厂商的应急响应部门以收录自身业务和产品的漏洞及威胁信息为主要目的和工作内容。收录方式主要有两种：一是通过自建应急响应平台在线收录，一是将指定邮箱或新浪微博、腾讯公共账号设置为统一的收录接口。同时，部分应急响应部门还会定期或不定期地发布漏洞处置情况及最新工作动态。

为了吸引更多负责任的安全研究人员发现、提交自家厂商的安全漏洞和威胁信息，绝大部分应急响应部门推出了多种方式的奖励和激励机制，并收到很好的效果。这类安全研究人员又称为“白帽子”，他们发现计算机系统或网络系统中的安全漏洞，但并不会去恶意利用和草率公布。例如，腾讯安全应急响应中心网站显示，“2015 年共有 334 位安全从业人员协助腾讯应急响应中心发现和修复了大量漏洞，从而提升了腾讯自有安全系统的能力”，并“为每一位在 2015 年度为腾讯做出贡献的安全专家们准备了丰富的现金和礼品奖励”，其中漏洞发现数量最多的人员获得了 12 万元的最高奖励。根据奇虎公司 360 安全播报平台的

报道，2015 年 360 安全应急响应中心累计为白帽子发放了 100 万元的奖金和礼品，并宣布 2016 年会将奖励总额提高一倍，升至 200 万元。

5.4.3 发挥的作用

各厂商应急响应部门的迅速建立和发展，打通了厂商与“白帽子”之间的正规渠道，相应的漏洞奖励也使得更多的“白帽子”关注并协助厂商发现自身业务和产品的漏洞与风险，很大程度上提高了厂商的信息安全程度。可以说，应急响应部门的建立，降低了厂商发现、修复漏洞的成本，提高了“白帽子”群体的收入，使得厂商和“白帽子”实现了双赢，而厂商客户和消费者则因为厂商产品信息安全水平的提高而最终获益。

表 17　国内知名安全应急响应中心

序号	名称	网址
1	腾讯安全应急响应中心(TSRC)	http://security.tencent.com/
2	阿里巴巴安全应急响应中心(ASRC)	https://security.alibaba.com/
3	百度安全应急响应中心(BSRC)	http://sec.baidu.com/views/main/index.html
4	360 安全应急响应中心(360SRC)	http://security.360.cn/
5	网易安全应急响应中心(NESC)	http://aq.163.com/
6	新浪安全应急响应中心(SSRC)	http://sec.sina.com.cn/
7	金山安全应急响应中心(KSRC)	http://sec.kingsoft.com/
8	安全狗安全应急响应中心(SVRC)	http://security.safedog.cn
9	小米安全中心(XMSC)	https://sec.xiaomi.com/

10	搜狗安全应急响应中心(SSRC)	http://sec.sogou.com/
11	迅雷安全应急响应中心(XLSRC)	http://safe.xunlei.com/
12	欢聚时代安全应急响应中心(YYSRC)	http://security.yy.com
13	京东安全应急响应中心(JSRC)	http://security.jd.com/
14	苏宁安全应急响应中心(SNSRC)	http://security.suning.com/ssrc-web/index.jsp
15	1 号店安全应急响应中心(1SRC)	http://security.yhd.com/
16	唯品会安全应急响应中心(VSRC)	http://sec.vip.com/
17	携程安全应急响应中心(CSRC)	http://sec.ctrip.com/
18	去哪儿网安全应急响应中心(QSRC)	http://security.qunar.com/
19	滴滴出行安全应急响应中心(DiDiSRC)	http://sec.didichuxing.com/
20	同程安全应急响应中心(LYSRC)	https://sec.ly.com/
21	蚂蚁金服安全应急响应中心(AFSRC)	https://security.alipay.com/sc/afsrc/home.htm
22	平安集团安全应急响应中心(PSRC)	http://security.pingan.com/
23	点融网安全应急响应中心(DSRC)	http://security.dianrong.com/index
24	联想安全应急响应中心(LSRC)	http://lsrc.lenovo.com/index.htm
25	海康威视萤石安全应急响应中心(YSRC)	http://ysrc.ys7.com/
26	华为产品安全事件响应团队（PSIRT）	http://www.huawei.com /psirt
27	中兴通讯“白帽子奖励计划”	http://www.zte.com.cn/cn/about/corporate_citizenship/security/201405/t20140530_424338.html
28	深信服安全响应中心(SFSRC)	http://security.sangfor.com.cn/index.php

六、总结与展望

2015 年，在依法治理网络、净化网络的同时，我国出台了一系列网络和信息安全相关的法律法规、指导文件和标准，使得信息安全总体政策环境明显改善，网络安全与信息化双轮驱动，技术发展与监管并驾齐驱。2015 年 6 月，第十二届全国人大常委会第十五次会议初次审议了《中华人民共和国网络安全法（草案）》，并面向社会公开征求意见，表明此项工作进入新的发展阶段。

漏洞是网络信息安全事件发生的根本原因之一，对漏洞的研究、分析、消除能力，很大程度上反映了一个国家的信息安全水平。近几年，随着新技术、新应用的不断涌现与普及，以“互联网+移动互联网+物联网”为信息传输和采集途径、以云存储和云计算为手段、以大数据为核心基础的新一代互联网体系，对我国现有的信息安全保障能力提出了巨大挑战。国家基础信息网络与重要信息系统的核心要害部位技术产品过度依赖国外的情况尚未根本改变；电子政务系统因为漏洞的存在而依然很脆弱，由漏洞攻击引起的失窃密事件和大规模数据泄露事件不断发生；通过漏洞而实现的 APT 攻击明显增加，对生产生活造成严重威胁等等。与许多国外发达国家和信息安全强国相比，我国对漏洞的研究、分析能力还要大力加强。

同时，国家级战略“互联网+”行动计划，必将使互联网市场这一新兴市场高速增长。面对诸如互联网金融、移动交易、移动支付等新业务，如何解决爆炸式的互联网业务的安全需求增长和相对滞后的安全保障发展之间的矛盾，如何保障安全而有序的“大众创业、万众创新”，是摆在每一个信息安全行业从业人员面前的重要问题。

可以预测，2016 年漏洞数量尤其是高危漏洞数量将继续呈现持续增长的态势，高危漏洞也将延续移动终端化的特点。由漏洞引发的各种威胁风险也将持续增加，利用漏洞进行攻击的类型将快速更新，信息泄露、系统篡改等事件将继续

高发。云计算、物联网、移动互联网、大数据、智慧城市等近几年的热点技术也将继续保持“高温”，各行业和地方建设基于云计算的应用平台、大型数据中心和大数据分析系统将持续实施，随着安全研究人员对其关注度的日益增加，相关漏洞也将居高不下会被不断披露，高危漏洞和安全事件的不断曝光将难以避免，所带来的威胁和损失将更加严重。

展望未来，国家将在高度重视网络信息安全问题的同时，相应的政策、法规及制度等工作必将持续推出。技术研发、项目投入、人才培养为解决信息安全漏洞问题提供了有力支撑。同时在企业、用户、专家等各方共同参与和努力下，该项工作必将得到有效推进。

附：国家信息安全漏洞库简介

国家信息安全漏洞库，英文名称"China National Vulnerability Database of Information Security "，简称"CNNVD"，是中国信息安全测评中心为切实履行漏洞分析和风险评估的职能，负责建设运维的国家信息安全漏洞库，为我国信息安全保障提供基础服务。

邮箱：vulpro@itsec.gov.cn

电话：010-82341439 / 010-82341409

官网：http://www.cnnvd.org.cn/

微信公众号

官方微博