信息安全漏洞通报

(2015 年 12 月)

根据国家信息安全漏洞库（CNNVD）统计，2015 年 12 月份新增安全漏洞共 694 个，从厂商分布来看， Adobe 公司产品的漏洞数量最多，共发布 99 个；从漏洞类型来看，缓冲区溢出类的漏洞占比最大，达到 21.61%。本月新增漏洞中，危急漏洞 87 个、高危漏洞 204 个、中危漏洞 372 个、低危漏洞 31 个，相应修复率分别为 97.70%、95.10%、81.99%以及 87.10%。合计 611 个漏洞已有修复补丁发布，本月整体修复率 88.04%。

截至 2015 年 12 月 31 日，CNNVD 收录漏洞总量已达 80329 个。

一、漏洞增长概况

12 月 Apple、Adobe、Google 等厂商漏洞数量大幅度增加，导致本月新增安全漏洞数量与上月相比有所上升。上述几个大型厂商发布漏洞的数量很大程度上左右了近三个月的漏洞走势，包括 10 月漏洞数量的激增、11 月漏洞数量的大幅度下降、以及 12 月漏洞数量的回升。图 1 为近 6 个月来漏洞新增数量统计图。

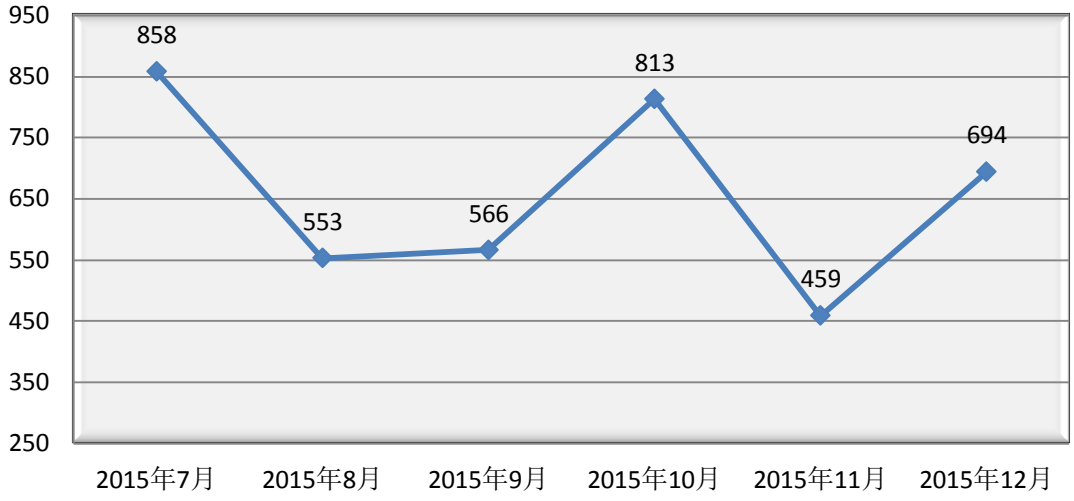

图 1　2015 年 7 月至 2015 年 12 月漏洞新增数量统计图

二、 漏洞分布情况

漏洞厂商分布

12 月厂商漏洞数量分布情况如表 1 所示，Adobe 公司达到 99 个，占本月漏洞总量的 14.27%，涉及 Adobe Flash Player、Adobe AIR SDK 等多款产品，全部是高危级别漏洞且已全部修复，希望用户及时更新补丁修复漏洞。

表 1　2015 年 12 月排名前十厂商新增安全漏洞统计表

序号	厂商名称	漏洞数量	所占比例
1	Adobe	99	14.27%
2	Apple	71	10.23%
3	Microsoft	58	8.36%
4	Google	55	7.93%
5	Cisco	45	6.48%
6	IBM	25	3.60%
7	Mozilla	24	3.46%
8	WordPress	14	2.02%
9	Xen	11	1.59%
10	Huawei	9	1.30%

漏洞产品分布

1、　主流操作系统漏洞

12 月几款主流操作系统的漏洞统计情况如表 2 所示（由于 Windows 整体市占率高达百分之九十以上，所以下表针对不同的 Windows 版本分别进行统计）。本月 Windows 系列操作系统漏洞数量共 15 条，其中桌面操作系统 14 条，服务器操作系统 12 条。本月 iOS 漏洞数量大幅上升，达到 50 个，占主流操作系统漏洞总量的 27%，排名第一。Android 漏洞数量也呈现较大的增长，相当于 11 月的 2

倍多。可见本月安全研究人员和黑客对于移动操作系统的关注度较高。

表 2　2015 年 12 月主流操作系统漏洞数量统计

序号	操作系统名称	漏洞数量
1	iOS	50
2	Mac OS X	44
3	Android	23
4	Microsoft Windows Server 2008	11
5	Microsoft Windows Vista	11
6	Microsoft Windows 7	11
7	Microsoft Windows 8	10
8	Microsoft Windows Server 2012	9
9	Microsoft Windows 10	8
10	Linux kernel	8

2、　Web 浏览器漏洞数量统计

下图为 12 月各主要 Web 浏览器漏洞数量统计。本月主流浏览器漏洞数量大幅上升，达到 94 个，是 11 月漏洞数量的近 2 倍。本月 Google Chrome 漏洞数量激增，超过 Microsoft Internet Explorer 排名第一，达到 32 个，占主流浏览器漏洞的 34.04%；Internet Explorer 和 Mozilla Firefox 漏洞数量与上月相比波动较小，分别为 28 个和 21 个；上月未曝出漏洞的 Apple Safari 本月公布 13 个漏洞，占主流浏览器的 13.83%。

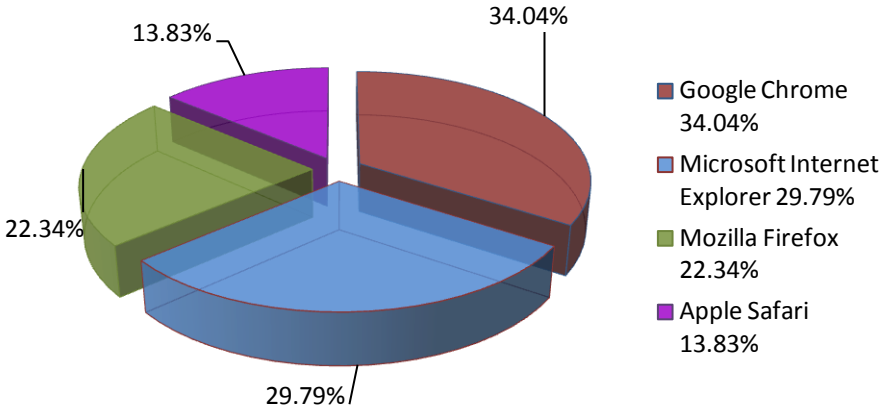

图 2　2015 年 12 月 Web 浏览器漏洞数量统计

漏洞类型分布

12 月份发布的漏洞类型分布如表 3 所示，其中缓冲区溢出类漏洞所占比例最大，约为 21.61%。缓冲区溢出漏洞是近来出现非常频繁、且后果严重的漏洞，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，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。

表 3　2015 年 12 月漏洞类型统计表

序号	漏洞类型	漏洞数量	所占比例
1	缓冲区溢出	150	21.61%
2	信息泄露	85	12.25%
3	权限许可和访问控制	67	9.65%
4	输入验证	55	7.93%
5	跨站脚本	38	5.48%
6	数字错误	21	3.03%
7	资源管理错误	17	2.45%
8	跨站请求伪造	14	2.02%
9	SQL 注入	13	1.87%
10	代码注入	11	1.59%
11	路径遍历	8	1.15%

12	授权问题	7	1.01%
13	信任管理	6	0.86%
14	加密问题	4	0.58%
15	竞争条件	4	0.58%
16	操作系统命令注入	2	0.29%

漏洞危害等级分布

根据漏洞的影响范围、利用方式、攻击后果等情况，从高到低可将其分为四个危害等级，即危急、高危、中危和低危级别。12 月漏洞危害等级分布如图 3 所示，其中危急漏洞 87 条，占总数的 12.54%，是 11 月的近 5 倍，危急漏洞数量和占比的增加表明 12 月安全威胁形势严峻。

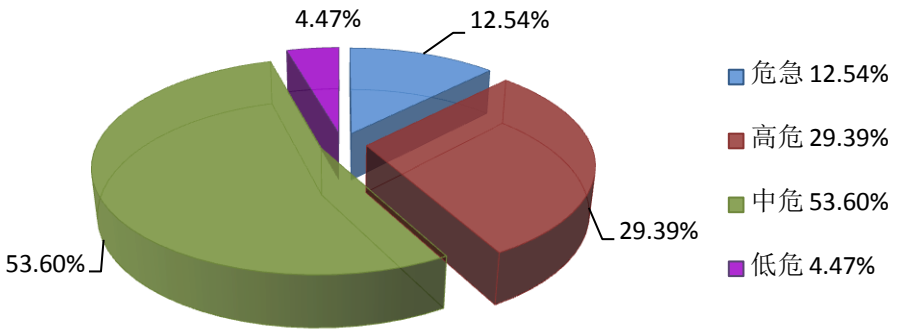

图 3　2015 年 12 月漏洞危害等级分布

三、 漏洞修复情况

整体修复情况

12 月漏洞修复情况按危害等级进行统计见图 4，危急漏洞修复率最高，比例为 97.70%，中危漏洞修复率最低，比例为 81.99%，本月危急、高危和低危漏洞的修复率都存在不同的涨幅，中危漏洞修复率

稍有下降，导致 12 月份漏洞整体修复率为 88.04%，环比增长了 3.61%。

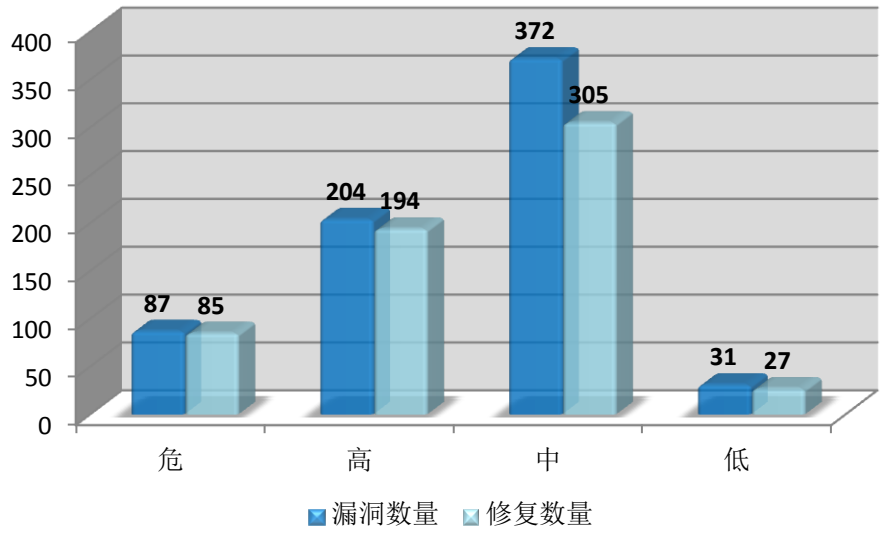

图 4　2015 年 12 月漏洞修复数量统计

厂商漏洞修复情况

12 月漏洞修复情况按漏洞数量前十厂商进行统计，多数知名厂商对产品安全高度重视，产品漏洞修复比较及时，其中 Apple、Microsoft、Google、Mozilla、Huawei 等公司共 316 条漏洞已全部修复，占本月漏洞的 45.53%。详细情况见表 4。

表 4　2015 年 12 月厂商修复情况统计表

序号	厂商名称	漏洞数量	修复数量	修复率
1	Adobe	99	99	100.00%
2	Apple	71	71	100.00%
3	Microsoft	58	58	100.00%
4	Google	55	55	100.00%
5	Cisco	45	31	68.89%
6	IBM	25	24	96.00%
7	Mozilla	24	24	100.00%
8	WordPress	14	11	78.57%
9	Xen	11	10	90.91%
10	Huawei	9	9	100.00%

四、本月重要漏洞实例

(一) 危急漏洞实例

本月危急漏洞共 87 个，其中重点漏洞实例如表 5 所示。

表 5　2015 年 12 月危急漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例
1	缓冲区溢出	CNNVD-201512-469	Mozilla	多款 Adobe 产品基于栈的缓冲区溢出漏洞 (CNNVD-201512-286)
		CNNVD-201512-286	Adobe	
		CNNVD-201512-071	Google	
		CNNVD-201512-542	Schneider Electric	
2	信任管理	CNNVD-201512-006	Saia Burgess Controls	ReadyNet WRT300N-DD Wireless Router 信任管理漏洞 (CNNVD-201512-319)
		CNNVD-201512-319	ReadyNet	
		CNNVD-201512-555	LOYTEC	
3	权限许可和访问控制	CNNVD-201512-601	Corega	Apple OS X File Bookmark 组件权限许可和访问控制漏洞（CNNVD-201512-360）
		CNNVD-201512-360	Apple	
4	数字错误	CNNVD-201512-471	Mozilla	Mozilla Firefox 和 Firefox ESR 整数溢出漏洞（CNNVD-201512-471）
5	授权问题	CNNVD-201512-540	Juniper Networks	Juniper Networks ScreenOS 授权问题漏洞（CNNVD-201512-540）

(二)　高危漏洞实例

本月高危漏洞共 204 个，其中重点漏洞实例如表 6 所示。

表 6　2015 年 12 月高危漏洞实例

序号	漏洞类型	漏洞编号	厂商	漏洞实例
1	缓冲区溢出	CNNVD-201512-365 CNNVD-201512-371	Apple	Google Chrome V8 缓冲区溢出漏洞

		CNNVD-201512-045	Google	（CNNVD-201512-045）
		CNNVD-201512-120	Microsoft	
		CNNVD-201512-275	Adobe	
2	权限许可和访问控制	CNNVD-201512-556	EMC	SAP Mobile Platform SysAdminWebTool servlets 权限许可和访问控制漏洞（CNNVD-201512-515）
		CNNVD-201512-099	Google	
		CNNVD-201512-515	SAP	
3	信息泄露	CNNVD-201512-032	Cyru	Honeywell International Midas 和 Midas Black 信息泄露漏洞（CNNVD-201512-036）
		CNNVD-201512-036	Honeywell International	
4	SQL 注入	CNNVD-201512-004	Epiphany Healthcare	Epiphany Healthcare Cardio Server SQL 注入漏洞（CNNVD-201512-004）
5	竞争条件	CNNVD-201512-486	ISC	ISC BIND named 竞争条件漏洞（CNNVD-201512-486）

注：本报根据中国国家信息安全漏洞库（CNNVD）数据整理分析而成，相关数据以本报发布的日期为准。

国家信息安全漏洞库

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：82341439

中国信息安全测评中心

中国信息安全测评中心成立于 1997 年，是我国专门从事信息技术安全测试和风险评估的权威职能机构。依据中央授权，测评中心的主要职能包括：负责信息技术产品和系统的安全漏洞分析与信息通报；负责党政机关信息网络、重要信息系统的安全风险评估；开展信息技术产品、系统和工程建设的安全性测试与评估；开展信息安全服务和专业人员的能力评估与资质审核；从事信息安全测试评估的理论研究、技术研发、标准研制等。

地址：北京市海淀区上地西路 8 号院 1 号楼

邮编：100085

电话：82341439

传真：82341100