DOI:10.16280/j.videoe.2014.16.023

【本文献信息】何晶.基于WooYun的视听新媒体网站漏洞统计分析[J].电视技术,2014,38(16).

基于WooYun的视听新媒体网站漏洞统计分析

何 晶
(广播科学研究院互联网技术研究所,北京 100866)

【摘 要】漏洞库是重要的信息安全基础设施,上面保存了大量网站信息安全风险样本。视听网站作为重要的信息发布平台,其信息安全性应受到极大的重视。通过对视听网站在乌云漏洞库(WooYun)中的漏洞信息进行统计分析,从漏洞数量、提交时间、危害等级和漏洞类型等方面进行多角度分析,发现其中一些共性的特点和问题,为我国视听领域的信息安全发展提供建议和参考。

【关键词】视听网站;漏洞库;统计分析;乌云漏洞库
【中图分类号】TN948 【文献标志码】A

Statistical Analysis of Audiovisual Newmedia Website Vulnerability Based on WooYun Vulnerability Database

HE Jing
(*Academy of Broadcasting Science Internet Technology Institute, Beijing 100866, China*)

【Abstract】Vulnerability database is an important information security infrastructure, it holds a large number of various types web security vulnerability. Audiovisual website as an important platform for information prorogation, the security should be of pay attention to. This paper is based on the WooYun vulnerability database for statistical analysis, through multi-angle analysis from the number of vulnerabilities, from reporting time, the degree of harm and vulnerability types, etc., and try to find some common problems. And it indicates some useful & interesting advice and information in the field of audiovisual website security.

【Key words】audiovisual website; vulnerability database; statistical analysis; WooYun

近年来,漏洞库成为重要的信息收集和发布平台,这对分析漏洞的分布、发展趋势提供了很好的样本空间。本文选取主要的视听网站作为研究对象,通过对乌云漏洞库(WooYun.org)中视听节目服务网站各种漏洞信息进行分析和汇总,从数量、报告时间、危害等级和漏洞类型等角度,总结出一些现象和特征,为我国网络视听领域中的信息安全提供建议和参考。

1 乌云漏洞库分析

1.1 漏洞库简介

漏洞库是为更好地进行信息安全漏洞的管理及控制工作而建立的。乌云漏洞库是一个国内非官方的漏洞报告平台,同国家信息安全漏洞共享平台(China National Vulnerability Database,CNVD)、中国国家信息安全漏洞库(China National Vulnerability Database of Information Security,CNNVD)和美国著名的国家漏洞数据库(National Vulnerability Database)等漏洞库一样,设立的初衷是为了能够增强互联网网站的信息安全建设,其共同特点是数据资源丰富、漏洞描述全面详尽。在对网站进行安全风险评估的过程中,漏洞作者会发现一些有价值的现象或问题,向漏洞库进行提交,而漏洞库根据平等、公开和中立等原则,对收到的漏洞信息进行编号、分类和评级,对外进行公布。

为了更好地呈现漏洞信息,笔者从漏洞的信息页面梳理出乌云漏洞库标识与描述方法——乌云漏洞库元数据,如图1所示,与中国有效管理安全漏洞的基础标准GB/T 28458—2012《信息安全技术 安全漏洞标识描述规范》[1]作对照。在国家标准中,安全漏洞描述项包括标识号、名称、发布时间、发布单位、类别、等级、影响系统等必需的描述项,并可根据需要扩充(但不限于)相关编号、利用方法、解决方案建议、其他描述等描述项[2]。其中从重要性上来说,发布时间、类别和等级是漏洞的3个重要属性。如表1可以看出,乌云漏洞库元数据不仅根据标识描述规范在其他描述中添加了漏洞作者、Tags标签、厂商回复、最新状态、漏洞状态、披露状态,对必选描述项的发布时间、等级和利用方法也进行扩充,使得漏洞在描述、处理和反馈各个环节的描述更为完整。

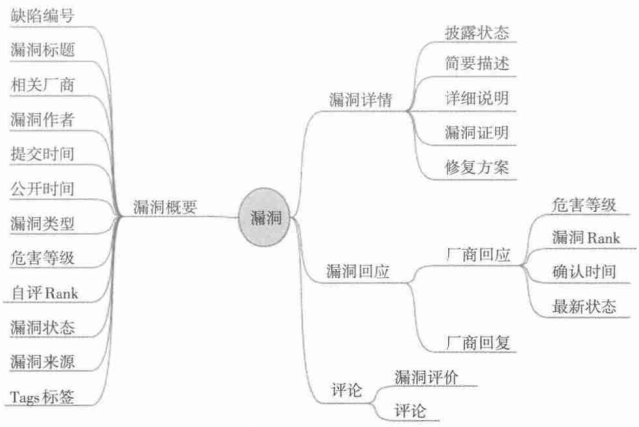


图1 乌云漏洞信息元数据

表1 安全漏洞标识描述与乌云漏洞库元数据的对应关系

安全漏洞标识描述规范描述项	乌云漏洞库元数据
标识号	缺陷编号
名称	漏洞标题
发布时间	提交日期、公开日期、确认时间
等级	危害等级、自评Rank（乌云网站定义的定量评价数值，取1~20之间的任意整数）、漏洞Rank
类别	漏洞类型
利用方法	简要描述、详细描述、漏洞证明
解决方案建议	修复方案
发布单位	漏洞来源
影响系统	相关厂商
相关编号	无
其他描述	漏洞作者、Tags标签、厂商回复、最新状态、漏洞状态、披露状态

对于乌云漏洞库元数据，改进的部分在于关联信息，对应国标的相关编号部分没有对应元数据。而且实践中也出现不少相关漏洞，如缺陷编号WooYun-2012-08336和WooYun-2012-12782，同样在survey.tudou.com/iresearch处报告Struts2命令执行漏洞，因此为了更好地完善漏洞描述，建议增加相关漏洞等关联信息。

1.2 视听网站选取

为了简化分析，本文只考虑独立视频网站，排除门户旗下网站（腾讯视频、搜狐视频、新浪视频）。根据反向链接数、PageRank等指标，按照网站价值的高低，选取优酷、土豆、PPTV、爱奇艺、CNTV、酷6、56网和乐视等共8家。

2 漏洞分析

2.1 漏洞数量和确认情况分析

截至2013年12月底，如表2所示，这8家网站共有554项漏洞被提交，共有482项优酷被网站确认，72项漏洞被忽略，整体确认率达到87%。

表2 各视听网站漏洞数量汇总
（提交日期截至2013年12月31日）

对比项	优酷	土豆	PPTV	爱奇艺	CNTV	酷6	56网	乐视	总数
漏洞总数	116	114	61	32	55	42	30	104	554
确认漏洞数量	103	78	58	31	48	32	30	102	482
忽略漏洞数量	13	36	3	1	7	10	0	2	72
确认率/%	88	68	95	96	87	76	100	98	87

对于72个忽略漏洞处理，分为几个不同情况，除了网站无回应无法分析忽略原因，54%的忽略漏洞被乌云追加Rank，这些漏洞平均Rank达到了5.88，这说明有很多低危害性的漏洞被网站选择性忽略。著名的TJX信息泄露事件，2006年美国零售业巨头TJX公司遭到黑客攻击，导致9 400万张信用卡和借记卡被盗。可以看出，攻击者会从不起眼的漏洞开始，绕过任何看似坚不可摧的网络隔离，最后几乎完全攻破关键性运营设备[3]。还有超过10%的忽略漏洞是由于漏洞作者提交的漏洞信息不全或提交对象与漏洞属主不符导致漏洞被忽略，这说明漏洞作者在信息收集阶段做的工作还不太到位。此外漏洞被忽略的情况还有网站认为问题不大、网站误操作和被白帽子（信息安全领域的安全研究人员，如漏洞作者和乌云网站的注册用户）发现网站自行修复。其中网站误操作和被白帽子发现网站自行修复对漏洞作者的积极性影响较大，建议网站能认真对待。忽略漏洞的处理情况如图2所示。

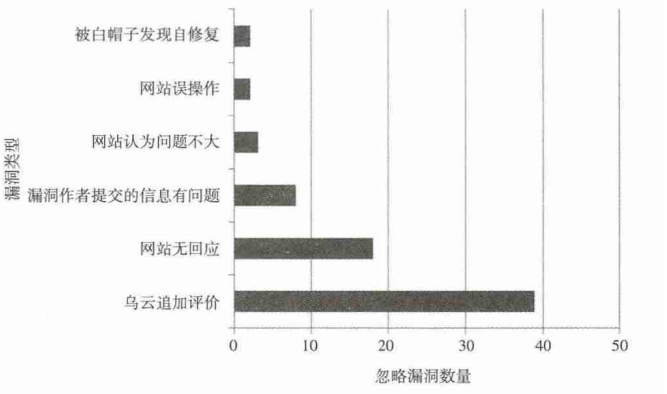


图2 忽略漏洞的处理情况

因此，视听网站应继续保持较高的漏洞确认率，但还要对低危害漏洞予以积极确认，而漏洞作者应准确描述漏洞，便于网站漏洞处置。

2.2 漏洞危害等级分析

漏洞的危害等级是漏洞属性的重要因素之一，根据漏洞评估结果的多样性，可以将漏洞评价技术划分为‘定性评级’和‘定量评分’。所谓定性评级即根据漏洞威胁评估要素，给漏洞确定一个威胁等级；定量评分

则根据既定的评分因素，给漏洞一个确定的威胁分值[4]。乌云的漏洞等级评价系统采用了“定性评级”和“定量评分”双重评价的方法。其中“定性评级”分为高、中、低3个级别；“定量评分”，定义为1~20之间的任意整数的Rank值。相比采用定性定量相关联(CVSS Severity)的美国国家漏洞库，乌云没有给出评分分值与定性评级的对应关系。此外乌云又允许漏洞作者、厂商和乌云追加三个评价角色，这样一个漏洞出现了4个评价结果：自评危害等级、自评Rank、网站评价危害等级和网站评价Rank(包含乌云追加)。这种做法既综合了定性评级的直观以及定量评分的客观，又不偏向漏洞作者和厂商任何一方，做到直观、客观和中立，但牺牲了一定的评价结果简单性。

本文为了统计方便，将危害等级根据低中高映射成1分、2分、3分。若网站忽略漏洞，则无网站评价危害等级和评价Rank。若网站忽略漏洞但乌云补评定没有危害等级，则只计入网站评价Rank，这里网站明确说明误操作的除外。

对各家漏洞等级进行统计，如表3所示，不论是危害等级还是Rank，平均来看漏洞作者自评比网站评价高，但没有出现NVD中等级为“高”的漏洞所占比例过高的现象[5]。基本维持在中级别(平均分2.23和2.17)和Rank为10(11.29和9.99)的平均线附近。这说明不论是漏洞作者还是网站，两方均认为目前整体的漏洞危害程度没有达到非常严重的阶段。而且网站对自身漏洞危害等级和Rank值的方差均比漏洞作者设定的差异要大，说明和漏洞作者群体相比，网站安全人员对漏洞的危害性评估会结合业务危害性情况给出不同结果，而笔者可以认为漏洞作者的自评对于漏洞的技术危害性评定较为统一。

表3 漏洞危害等级统计表

对比项	优酷	土豆	PPTV	爱奇艺	CNTV	酷6	56网	乐视	平均	方差
自评危害等级	2.06	2.02	2.28	2.34	2.35	2.21	2.10	2.45	2.23	0.024
自评Rank	10.63	10.07	11.20	11.81	11.87	11.60	10.67	12.45	11.29	0.62
网站评价危害等级	2.26	2.09	1.88	1.97	2.60	2.12	2.13	2.46	2.19	0.058
网站评价Rank	11.02	8.07	8.05	7.66	13.25	8.86	9.38	13.87	10.02	5.89

此外，危害等级比漏洞作者自评要高的5家网站(优酷、土豆、CNTV、56网和乐视)的漏洞数量占比75%。尽管Rank平均值网站明显低于漏洞作者自评，但是给出Rank高于漏洞作者的3家网站(优酷、CNTV和乐视)的漏洞数量占比也达到了50%。说明通常漏洞作者收到的漏洞评价与自身预期不一致，会相应影响提交漏洞的积极性，因此为了能促进漏洞作者积极提交漏洞，视听网站还应积极想办法。

乌云的危害等级评定采用漏洞作者、网站和乌云追加三个角色，结合“定性评级”、“定量评分”双重评价方法，在牺牲了简单性的基础上努力做到直观、客观和中立。漏洞作者和网站均认为当前的安全形势没有达到非常严重的阶段。此外网站的评价会影响漏洞作者提交漏洞的积极性。

2.3 漏洞提交时间分析

漏洞的提交时间是漏洞属性的重要属性之一，本部分对漏洞的提交时间属性进行统计分析。

图3是8家视听新媒体网站收到的漏洞作者提交漏洞的数量月度走势。可以看出，提交漏洞的总数量在波动中呈不断上升趋势，而且分为起始阶段和稳定阶段，具体划分方法为每月稳定提交10个漏洞及以上，大致时间节点在2012年2月前后。进一步分析，如图4所示，漏洞提交月均数量进行统计，可看出提交漏洞的时间出现明显波峰波谷。波峰如6、7、9、10和11月，月均提交的漏洞数量超过20个，高于其他月份，这些对今后漏洞趋势预测起到一定的借鉴作用。

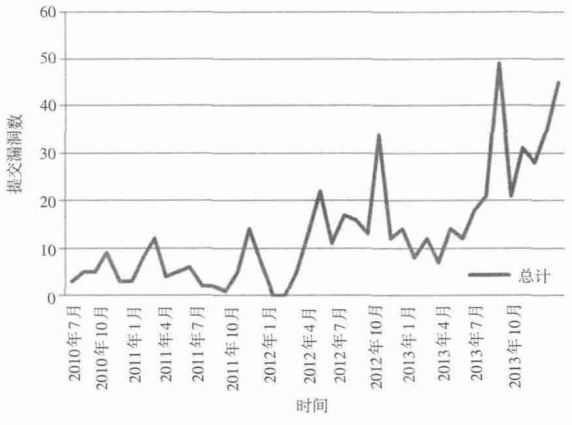


图3 漏洞提交数量月度走势图

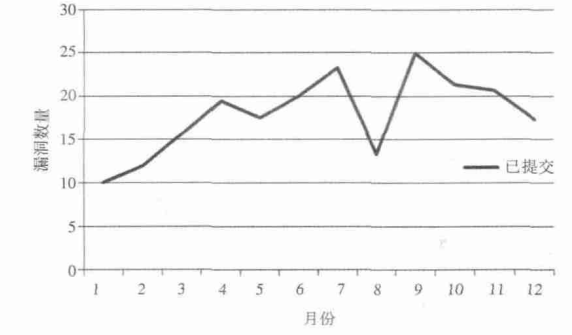
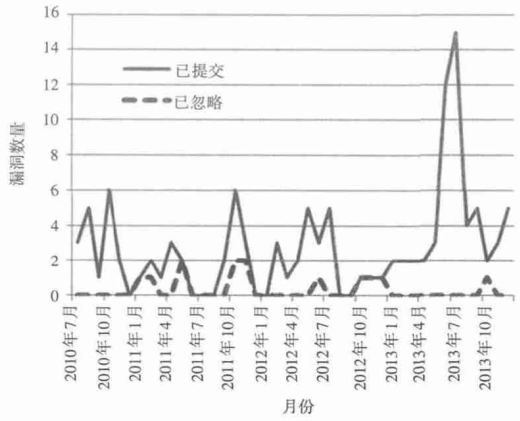
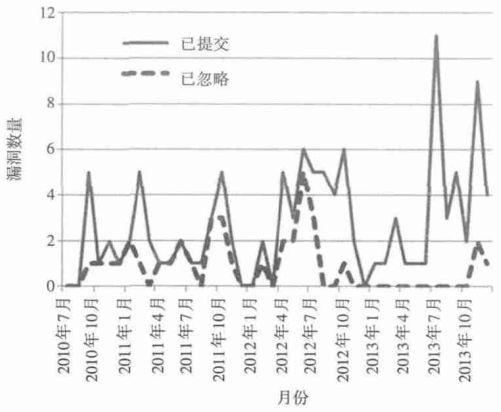


图4 漏洞提交数量月均统计图

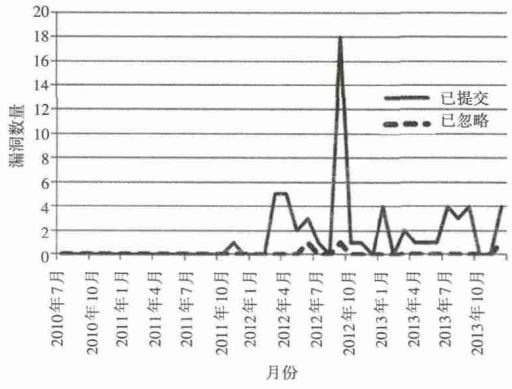
从单个视听网站的收到漏洞月度走势图进行进一步分析，如图5所示。重点在于长时间(大于等于6个月)没有漏洞报告和漏洞高发月份(单个网站单月收到超过10个漏洞)的情况。



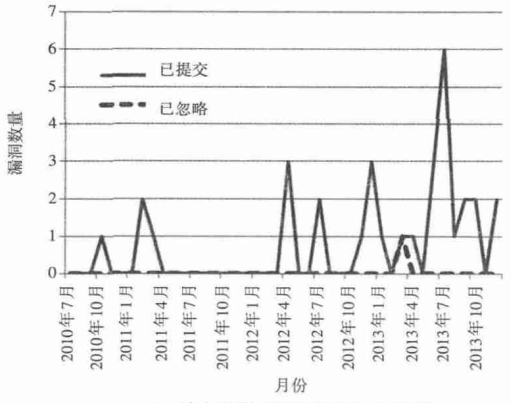
a 优酷收到漏洞月度走势图



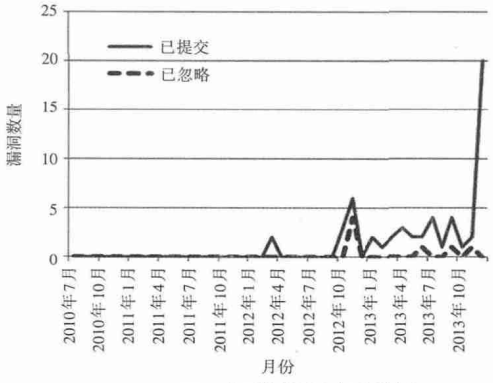
b 土豆收到漏洞月度走势图



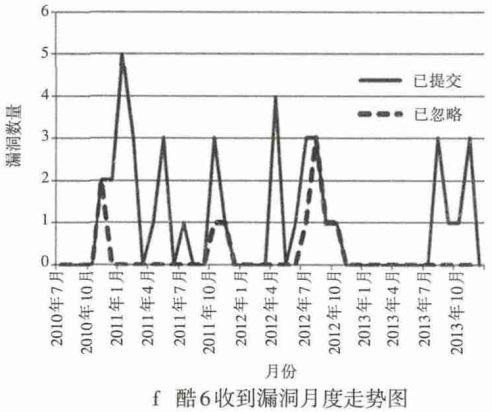
c PPTV收到漏洞月度走势图



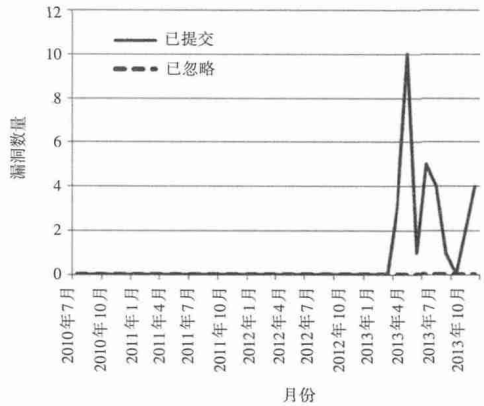
d 爱奇艺收到漏洞月度走势图



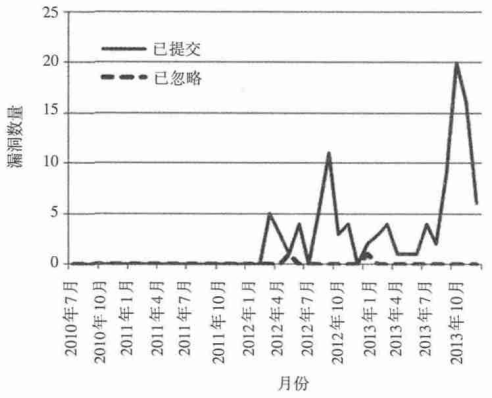
e CNTV收到漏洞月度走势图



f 酷6收到漏洞月度走势图



g 56网收到漏洞月度走势图



h 乐视收到漏洞月度走势图

图5 单个视听网站的收到漏洞月度走势图

这8家中，爱奇艺、CNTV和酷6长时间没有漏洞报告的情况。具体分析，爱奇艺和CNTV位于起始阶段，而酷6在稳定阶段。可理解为爱奇艺和CNTV开始有漏洞作者偶然发现漏洞并提交，后面不断有漏洞作者提交漏洞。而2012年7—9月一段时间内提交的漏洞被忽略后，白帽子长达9个月没有提交酷6的漏洞，长时间无漏洞和之前忽略漏洞呈现出一定的相关性，而且在当时白帽子评论中表示不满意该网站的安全响应机制，这对网站的信息安全风险的发现和处置产生了一定的影响。

结合图3和图5，漏洞高发月份的原因主要是单个网站的提交漏洞数量明显升高，如2012年9月，PPTV和乐视各收到18个和11个漏洞，两家共占当月85%，2013年7月优酷和土豆分别收到15个和11个，两家共占当月53%。进行进一步分析后发现，同类型漏洞的大面积爆发（如SQL注射漏洞、弱口令、命令执行）和漏洞作者的集中提交（PPTV 2012年9月）都可能会导致高发月份的出现。

因此，从提交时间属性分析，越来越多的视听网站漏洞被提交，希望网站的安全人员，特别是在高发月份段注意及时响应漏洞。此外同类型漏洞大面积爆发和漏洞作者集中提交这两个原因都有可能导致漏洞高发月份的出现，从客观条件和主观条件两方面都应注意。

各个网站漏洞高发月份成因如表4所示。

表4 各个网站漏洞高发月份成因

月份	漏洞数量（主要原因/总数）	网站	主要原因
2013年6月	7/12	优酷	敏感信息泄露/XSS跨站脚本攻击/SQL注射漏洞
2013年7月	8/15	优酷	SQL注射漏洞/XSS跨站脚本攻击
2013年7月	5/11	土豆	命令执行
2012年9月	10/18	PPTV	SQL注射漏洞/2013年9月10日提交13个漏洞
2013年12月	14/20	CNTV	SQL注射漏洞
2013年5月	5/10	56网	SQL注射漏洞
2012年9月	5/11	乐视	SQL注射漏洞
2013年10月	6/20	乐视	弱口令
2013年11月	8/15	乐视	弱口令/SQL注射漏洞

2.4 漏洞类型分析

类型也是漏洞的重要属性之一，乌云定义了6个大类型，29个小类型，视听网站至少报告了24种小类型。不同于《信息安全事件分类分级》国家标准中按事件行为将事件分成有害程序事件、网络攻击事件、信息破坏事件和信息内容安全事件等[6]，乌云是按基础架构、系统运维、应用程序、业务安全和安全事件等漏洞所处层次分成大类，再按技术描述细分小类型，会出现大类型不同小类型近似的问题。如敏感信息泄露、重要敏感信息泄露、网络敏感信息泄露3个类型实际上同属敏感信息泄露，服务弱口令和后台弱口令同为弱口令。为了更好说明问题，本文将按技术因素重新合并后形成17个类型，如图6所示。

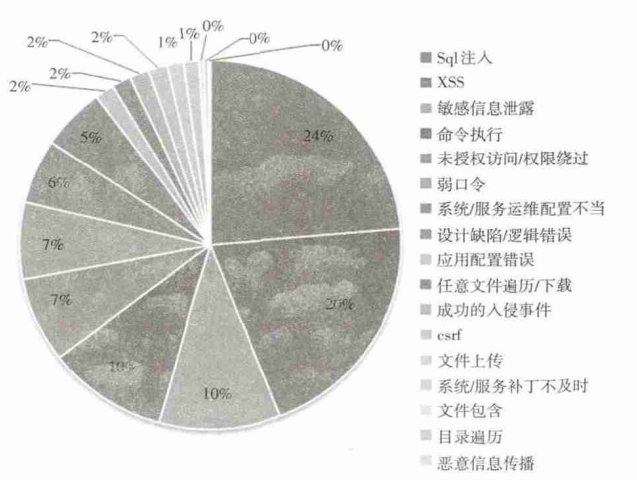


图6 视听网站漏洞类型分布图

可见SQL注入、XSS、命令执行和敏感信息泄露等传统漏洞占比64%，依然是主流问题。未授权访问/权限绕过、弱口令等账户管理漏洞占比17%，仍是很大的问题，特别是视听新媒体重要的专用系统，如乐视3个视频编码器后台弱口令高危害等级漏洞（缺陷编号WooYun-2013-43662，WooYun-2013-41663，WooYun-2013-41576），说明漏洞作者已开始对视听新媒体技术系统的业务安全重要性有一定的了解。此外由于配置问题导致的系统/服务运维配置不当、应用配置错误、系统/服务补丁不及时等配置问题占比9%，也暴露出网站运维过程管理的问题。通过评论也可以发现，一些漏洞的出现与系统的上线、更新有关。

结合之前提交日期中对高发月份的漏洞类型分析，确定漏洞的主要技术问题集中在传统的Web安全漏洞、账户和配置管理问题。

3 总结与展望

通过本文的分析发现，视听新媒体网站收到漏洞的数量在不断增长，这说明该领域的安全形势依然很严峻。漏洞类型方面应注意传统漏洞、账户和配置管理问题，这需要在运维管理中加强安全方面的管理。此外希望网站能及时响应漏洞，认可漏洞作者的辛勤

（下转第75页）

行相应封装，使拘束传播更为规范，从而实现高质量的网络组播。TS流通过IP组播后，应用性更加灵活，可以不受区域和时间限制，进行节目的录制和监理，操作极为便捷。一般多数据流对于带宽质量有要求，所以千兆以太网已成为该平台运行基础。

2.3.3 嵌入式系统构架

该设计具有高度集成特点，灵活性明显，机箱构架简约，具有良好的布局模式。机箱以4块不同功能模块为满配，模块装载以后运行，热插拔功能良好，模块之间均配置独立接口，配备电源备份。该设计有利于系统的维护、运行以及升级需要，而且还保证了不同类型模块与机箱的兼容性。

3 总结

该系统的核心监测设计均采用FPGA+DSP构架，该设计能够保证系统运行的稳定性，并能够提升数据处理性能，使硬件优势更为明显。

该系统于2013年12月安装调试完成后投入使用，各项性能指标都达到了设计要求。

参考文献：

[1] GY/T 170—2001，有线数字电视广播信道编码与调制规范[S].2001.
[2] GY/T 221—2006，有线数字电视系统技术要求和测量方法[S].2006.
[3] GY/T 230—2008，数字电视广播业务信息规范[S].2008.
[4] GB/T 17975.1—2000，信息技术 运动图像及其伴音信号的通用编码第1部分 系统[S].2000.
[5] GB/T 17975.2—2000，信息技术 运动图像及其伴音信号的通用编码第2部分 视频[S].2000.

责任编辑：任健男 收稿日期：2014-03-26

（上接第52页）

的地理位置展示在地图上，实现客户故障的定位分析、各类客户数据的分析、辅助客户经理进行营销管理等功能。为曲靖广电网络分公司参与三网融合提供了先机，为分公司的业务扩展打下了坚实的基础。鉴于资源管理系统建设给广电网络带来的诸多好处，云南广电网络集团公司将建设覆盖云南全省的广电网络资源管理系统。

参考文献：

[1] 李新苗. 运营商综合网络资源管理进入新阶段[J]. 通信世界，2010(21)：35.
[2] 倪晨鸣，宋庆文. 广电网络资源管理系统建设模式探讨[J]. 有线电视技术，2008(3)：53-57.
[3] 任宁宁. 有线电视网络资源管理系统建设规则[J]. 电视技术，2013，37(4)：47-51.

作者简介：

张 毅（1961—），高级工程师，主要从事有线数字电视网络、无线传输网络方面的研究；

邹引凡（1957—），高级工程师，主要从事有线电视网络战略规划方面的研究；

张兴华（1965—），高级工程师，主要从事有线电视网络、干线传输方面的研究。

责任编辑：薛 京 收稿日期：2014-07-04

（上接第69页）

工作，提高漏洞作者的积极性。当然，相比上万条的通用漏洞信息库，本文分析的五百余条漏洞样本数量尚不足以说明对通用漏洞库上述分析是否有效。此外漏洞提交与响应时间的关系、漏洞作者的技术偏好、漏洞的Tag信息等方面还有待做进一步的分析。

参考文献：

[1] 刘奇旭，张玉清，宫亚峰，等. 安全漏洞标识与描述规范的研究[J]. 信息网络安全，2011(7)：4-6.
[2] 中国国家标准化管理委员会. GB/T 28458—2012，信息安全技术 安全漏洞标识与描述规范[S]. 北京：中国标准出版社，2012.
[3] ZALEWSKI M. Web之困 现代Web应用安全指南[M]. 朱筱丹，译. 北京：机械工业出版社，2013.
[4] 刘奇旭，张翀斌，张玉清，等. 安全漏洞等级划分关键技术研究[J]. 通信学报，2012，33(S1)：79-87.
[5] JONES J. CVSS severity analysis 2008[EB/OL]. [2014-01-27]. http://first.org/cvss/jones-jeff-slides.pdf.
[6] 中国国家标准化管理委员会. GB/Z 20986—2007，信息安全技术 信息安全事件分类分级指南[S]. 北京：中国标准出版社，2007.

责任编辑：任健男 收稿日期：2014-02-27