

信息安全漏洞周报

2014 年 9 月 29 日-2014 年 10 月 12 日

2014年第40、41期

本周漏洞基本情况

本周信息安全漏洞威胁整体评价级别为**高**。

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 188 个，其中高危漏洞 47 个、中危漏洞 129 个、低危漏洞 12 个。上述漏洞中，可利用来实施远程攻击的漏洞有 178 个。本周收录的漏洞中，已有 95 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。本周互联网上出现“Allo maniWeblinks 存在多个漏洞”、“HTTP File Server 远程命令执行漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。本周，针对 GNU Bash 的攻击或扫描呈上升趋势，采用 CGI 组件的网站成为攻击的重点目标，其中，多款邮件系统产品受到影响，构成信息泄露和运行安全的较大威胁。

成员单位报送漏洞统计

本周，共 6 家成员单位、合作伙伴及个人报送了本周收录的全部 188 个漏洞。报送情况如表 1 所示。其中，奇虎 360、天融信、安天实验室、启明星辰等单位报送数量较多。此外，CNCERT 各分中心、北京安赛创想科技有限公司、上海天泰网络技术有限公司及白帽子向 CNVD 提交了 715 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	684	684
天融信	418	0
安天实验室	208	0
启明星辰	96	0

绿盟科技	70	0
恒安嘉新	42	0
High-Tech Bridge Security Research Lab	5	5
北京安赛创想科技有 限公司	1	1
上海天泰网络技术有 限公司	1	1
CNCERT 陕西分中心	9	9
CNCERT 甘肃分中心	5	5
CNCERT 山西分中心	2	2
CNCERT 江西分中心	1	1
CNCERT 福建分中心	1	1
CNCERT 湖南分中心	1	1
CNCERT 宁夏分中心	1	1
个人	4	4
报送总计	1549	715
录入总计	188（去重）	715

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Google、Mozilla、HP 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Google	16	9%
2	Mozilla	13	7%
3	HP	11	5%
4	WordPress	6	3%
5	Linux	6	3%
6	Juniper	6	3%
7	OpenStack	4	2%
8	IBM	3	2%
9	Bugzilla	3	2%
10	其他	120	64%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周,CNVD 收录了 188 个漏洞。其中应用程序漏洞 130 个,WEB 应用漏洞 26 个,操作系统漏洞 17 个,网络设备漏洞 15 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	130
WEB 应用漏洞	26
操作系统漏洞	17
网络设备漏洞	15

表 3 漏洞按影响类型统计表

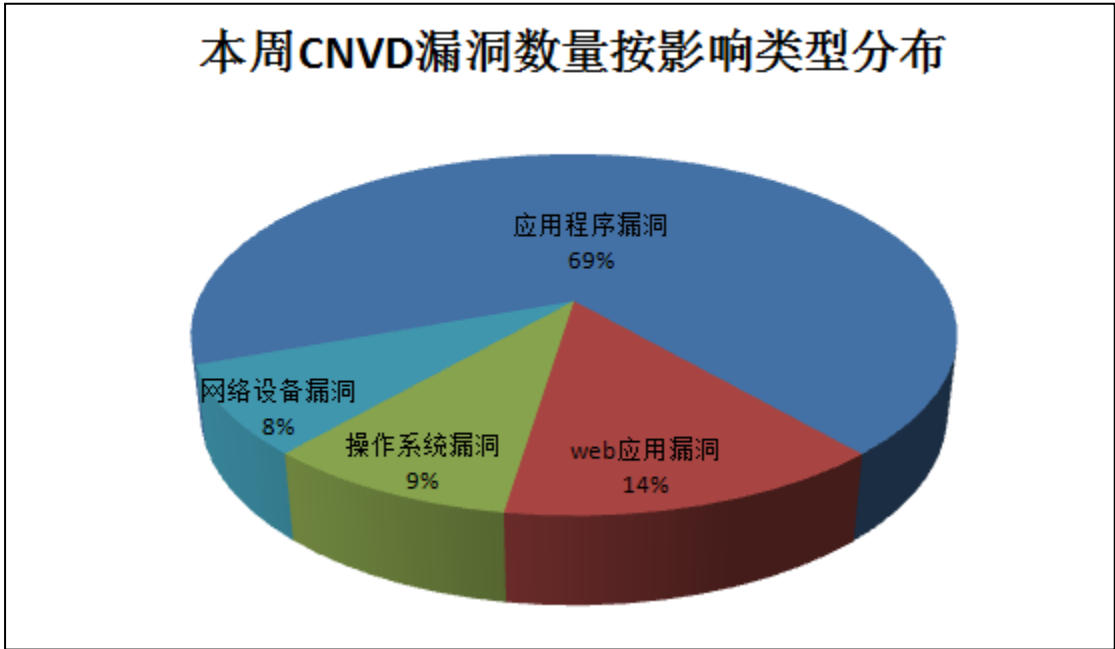


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周, CNVD 收录了 8 个电信行业漏洞, 49 个移动互联网漏洞 (如下图表所示)。其中, “Cisco IOS XR Software 安全绕过漏洞” 的综合评级均为 “高危”。相关厂商已经发布了上述漏洞的修补程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2014-06542	Modem Nucom ADSL R5000UN 信息泄露漏洞	中	否
电信	CNVD-2014-06557	Cisco WebEx Meetings Server 任意文件下载漏洞	中	是

电信	CNVD-2014-06555	Cisco IOS XR Software 安全绕过漏洞	高	是
电信	CNVD-2014-06577	TeamSpeak Client 缓冲区溢出漏洞 (CNVD-2014-06577)	中	否
电信	CNVD-2014-06578	TeamSpeak Client 缓冲区溢出漏洞 (CNVD-2014-06578)	中	否
电信	CNVD-2014-06598	NetCommWireless NB604N ADSL2+ Router 'wsecurity.html' HTML 注入漏洞	低	是
电信	CNVD-2014-06615	IBM WebSphere Portal 信息泄露漏洞 (CNVD-2014-06615)	中	是
电信	CNVD-2014-06630	Juniper JunosE ICMP 报文处理拒绝服务漏洞	中	是
移动互联网	CNVD-2014-06463	My Mobile Day for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06458	ITriage Health for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06459	Fastin for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06461	Designs Nail Arts for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06494	NBA Game Time 2013-2014 for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06493	Morocco Weather for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06492	Candy Girl Party Makeover for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06491	Wedding Photo Frames-Love Pics for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06490	5SOS Family Planet for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06489	Juiker for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06488	Kingsoft Clip (Office Tool) for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06487	UC Browser HD for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06486	InstaMessage - Instagram Chat for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06485	wsaudichannelalnas for android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06481	Amazigh Music for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06482	ChallengerTX for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06479	Friendcaster for Android SSL 信息泄露漏洞	中	否

移动互联网	CNVD-2014-06484	phonearabs4 for android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06483	StarSat International for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06480	ChatBox - Chat Rooms for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06497	Vendormate Mobile for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06501	Sporting Club Uphoria for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06498	Maher Zain for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06496	Utah Jazz for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06495	DreamlSuper Theme GO Gold for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06503	GrooveMusic for android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06506	MegaBank for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06505	Halieutics for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06504	Guess The Actor for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06502	Russiananime for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06500	BundesArztsuche for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06499	Tx Smart for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06515	The Weather Channel for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06516	Galaxy Online 2 for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06518	w88235ff7bdc2fb574f1789750ea99ed6 for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06524	iGolf - Golf GPS for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06526	WebMD for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06528	MoWeather for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06527	Genertel for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06525	healthylifestyle for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06561	SlotMachine for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06560	Medical Chat and MCQs for Android	中	否

		信息泄露漏洞		
移动互联网	CNVD-2014-06563	М а л е н ь к и й к о н ц е р т -B abyBus for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06566	Chifro Kids Coloring Game for Androi d SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06564	TechRadar News for Android SSL 信息 泄露漏洞	中	否
移动互联网	CNVD-2014-06565	Embry-Riddle for Android SSL 信息泄 露漏洞	中	否
移动互联网	CNVD-2014-06567	Airlines International for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06568	ABC Lounge Webradio for Android SS L 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06569	7Sage LSAT Prep - Proctor for Androi d SSL 信息泄露漏洞	中	否

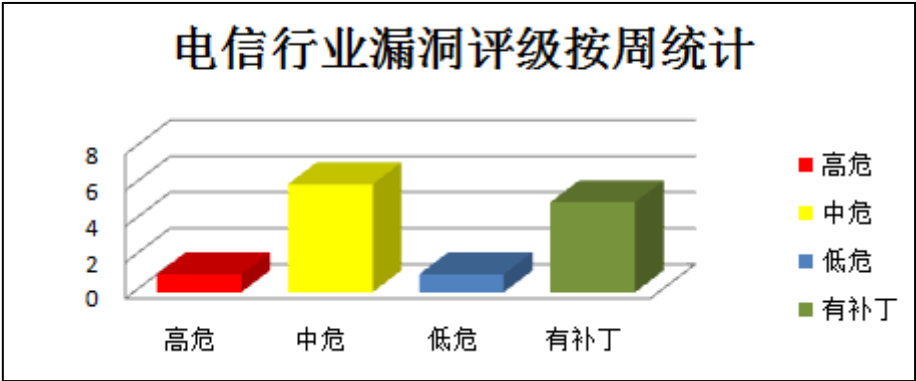


图 1 电信行业漏洞统计

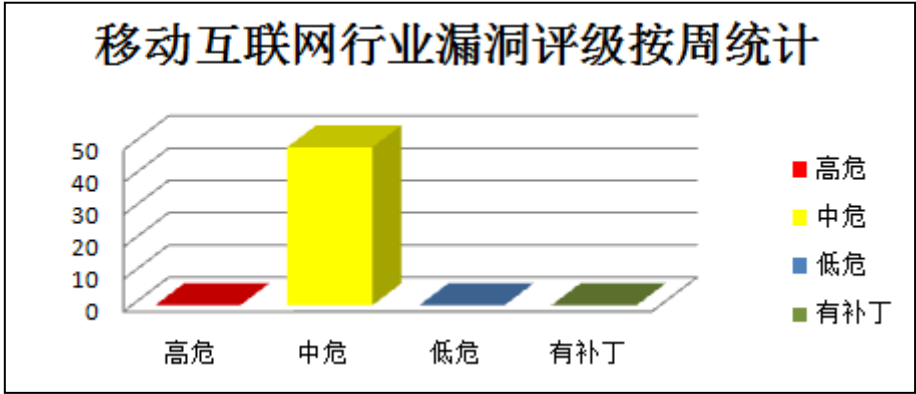


图 2 移动互联网行业漏洞统计

本周重要漏洞信息

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Google 产品安全漏洞

Google Chrome 是由 Google 开发的一款 Web 浏览工具。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Chrome 拒绝服务漏洞（CNVD-2014-06639）、Google Chrome 存在多个内存破坏漏洞、Google Chrome windows 沙盒权限绕过漏洞、Google Chrome 内存错误引用漏洞（CNVD-2014-06637）、Google Chrome DOM 内存错误引用漏洞（CNVD-2014-06638）、Google Chrome Events 内存错误引用漏洞、Google Chrome PDFium 越界读漏洞、Google Chrome V8 和 IPC 远程代码执行漏洞。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06639>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06551>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06570>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06637>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06638>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06636>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06635>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06634>

2、Mozilla 产品安全漏洞

Firefox/Thunderbird/SeaMonkey 是 Mozilla 所发布的 WEB 浏览器和邮件/新闻组客户端。本周，上述产品被披露存在多个远程漏洞，攻击者可利用漏洞获取敏感信息、执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird/SeaMonkey 存在多个远程漏洞（CNVD-2014-06462、CNVD-2014-06464、CNVD-2014-06465、CNVD-2014-06466、CNVD-2014-06467、CNVD-2014-06460、CNVD-2014-06469、CNVD-2014-06472）。上述漏洞的综合评级为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06462>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06464>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06465>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06466>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06467>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06460>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06469>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06472>

3、HP 产品安全漏洞

HP Sprinter 是一款为测试人员提供多种强大工具以运行手动测试的综合解决方案；HP Operations 是一款用于管理分散式环境的分散式用户端/服务软件产品；HP Systems Insight Manager(HP SIM)是 HP 公司推出的，偏重于 HP 服务器、存储等硬件管理的一套软件。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码、提升权限或进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：HP Sprinter 存在未明远程代码执行漏洞（CNVD-2014-06625、CNVD-2014-06624、CNVD-2014-06623、CNVD-2014-06622）、HP Operations Manager 存在未明远程代码执行漏洞、HP Systems Insight Manager 远程权提升漏洞、HP Systems Insight Manager 存在未明跨站脚本漏洞、HP Systems Insight Manager 存在未明点击劫持漏洞。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06625>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06624>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06623>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06622>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06621>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06596>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06594>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06595>

4、Juniper Networks 产品安全漏洞

Juniper Networks Junos 是美国瞻博网络（Juniper Networks）公司的一套专用于该公司的硬件系统的网络操作系统。本周，上述产品被披露存在拒绝服务和安全绕过漏洞，攻击者可利用漏洞发起拒绝服务和执行未授权操作。

CNVD 收录的相关漏洞包括：Juniper Junos 拒绝服务漏洞（CNVD-2014-06631、CNVD-2014-06627、CNVD-2014-06626、CNVD-2014-06629）、Juniper JunosE ICMP 报文处理拒绝服务漏洞、Juniper Junos 安全绕过漏洞。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06631>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06627>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06626>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06629>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06630>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06628>

5、TYPO3 JobControl 存在多个漏洞

TYPO3 是一个免费开源的内容管理系统。本周，TYPO3 JobControl 被披露存在综合评级为“高危”的 SQL 注入和跨站脚本漏洞。攻击者可利用漏洞危及应用程序，访问或修改数据。目前，厂商尚未发布该漏洞的修补程序。CNVD 提醒广大用户随时关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2014-06510>

更多高危漏洞如表 3 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。

参考链接：<http://www.cnvd.org.cn/flaw/list.htm>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2014-06522	Cobham Aviator 700D 及 700E 本地信息泄露漏洞	高	暂无
CNVD-2014-06533	多个 ManageEngine 产品存在任意文件上传漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.manageengine.com/it360/
CNVD-2014-06532	ManageEngineOpManager 存在任意文件上传漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.manageengine.com/products/service-desk/opmanager-integration.html
CNVD-2014-06535	Xen 拒绝服务漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.xenproject.org/
CNVD-2014-06537	ArubaOS 验证绕过漏洞	高	暂无
CNVD-2014-06562	Moab HPC Suite 安全绕过漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.adaptivecomputing.com/products/
CNVD-2014-06559	Bassmaster 'eval()'函数任意代码执行漏洞	高	Bassmaster 1.5.2 已经修复该漏洞，建议用户下载更新： https://www.npmjs.org/package/bassmaster
CNVD-2014-06579	GoPro HERO 3+ 'gpExec' start 远程代码执行漏洞	高	暂无
CNVD-2014-06580	GoPro HERO 3+ 'gpExec' restart 远程代码执行漏洞	高	暂无

CNVD-2014-06573	AutoWeb 'noticias.php' SQL 注入漏洞	高	暂无
-----------------	---------------------------------	---	----

表 3 部分高危漏洞列表

小结：本周，移动互联网行业漏洞数相对较多，主要原因是收录了多个 Android 应用程序存在的 SSL 证书验证漏洞，攻击者可利用漏洞获取敏感信息，请各应用软件方注意防范 Android SSL 证书验证漏洞。此外，Google Chrome 及 Mozilla、HP、JunioerNetworks 多款产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息，执行任意代码或发起拒绝服务攻击。另外，TYPO3 JobControl 被披露存在一个高危零日漏洞。攻击者可利用漏洞窃取 cookie 认证证书，危及应用程序，访问或修改数据。建议相关用户应随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、IBM 修补 WebSphere Portal、Rational ClearQuest 产品漏洞

IBM WebSphere Portal 提供了一个组合应用程序或业务 mashup 框架，并且提供了一种高级工具来构造灵活的基于 SOA 的解决方案；IBM Rational ClearQuest 是全面的软件变更、追踪管理解决方案。

本周，IBM 修补了上述产品存在的信息泄露和拒绝服务漏洞，避免攻击者利用漏洞获取敏感信息或发起拒绝服务攻击。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/50659>

<http://www.cnvd.org.cn/patchInfo/show/50579>

<http://www.cnvd.org.cn/patchInfo/show/50582>

本周要闻速递

1. Bash 漏洞再次演进：缓冲区溢出导致远程任意命令执行

CVE-2014-7187 是一个最新的 Bash 漏洞，根据官方的说明文档，其存在于 parse.y 中的 read_token_word 函数，可以通过构造可执行程序 BSS 字段产生漏洞，允许攻击者利用漏洞执行任意远程代码。目前已经有人分别在 Ubuntu14.04LTS 和 OSX 10.9.5 上验证了该漏洞。

参考链接：<http://www.freebuf.com/news/45436.html>

2. 雅虎贡献者网站被曝 SQL 注入漏洞

Behrouz Sadeghipour 通过盲注发现了雅虎贡献者网站存在一个 SQL 漏洞，该漏洞可能会使黑客利用来窃取用户和作者的个人信息。该漏洞于几个月之前被提交，雅虎修复之后便以知名度下降为理由关闭了贡献者网站。

参考链接：<http://sec.chinabyte.com/397/13104397.shtml>

关于 CNVD

国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

关于 CNCERT

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999