国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2014 年 9 月 22 日-2014 年 9 月 28 日　　2014 年第 39 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**中**。

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 346 个，其中高危漏洞 42 个、中危漏洞 279 个、低危漏洞 25 个。上述漏洞中，可利用来实施远程攻击的漏洞有 310 个。本周收录的漏洞中，已有 178 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“Joomla! Face Gallery 存在多个漏洞”、“ALCASAR 'index.php'不完整修复远程代码执行漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。

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 346 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、习科网络安全、国防科大计算机学院及白帽子向 CNVD 提交了 496 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	473	473
天融信	319	0
安天实验室	242	0
启明星辰	119	0
绿盟科技	95	0
恒安嘉新	82	0

High-Tech Bridge Security Research Lab	1	1
习科网络安全	1	1
国防科大计算机学院	1	1
CNCERT 江西分中心	13	13
CNCERT 新疆分中心	4	4
CNCERT 福建分中心	1	1
CNCERT 山西分中心	1	1
个人	1	1
报送总计	1353	496
录入总计	346（去重）	496

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Apple、WordPress、Cisco 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	Apple	64	18%
2	WordPress	15	4%
3	Cisco	14	4%
4	IBM	12	4%
5	Wireshark Foundation	12	3%
6	LibVNCServer	5	2%
7	Gnu	2	1%
8	X2Engine Inc.	2	1%
9	Microsoft	1	1%
10	其他	219	62%

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 346 个漏洞。其中应用程序漏洞 242 个，操作系统漏洞 59 个，WEB 应用漏洞 23 个，网络设备漏洞 22 个。

漏洞影响对象类型	漏洞数量

应用程序漏洞	242
操作系统漏洞	59
WEB 应用漏洞	23
网络设备漏洞	22

表 3 漏洞按影响类型统计表

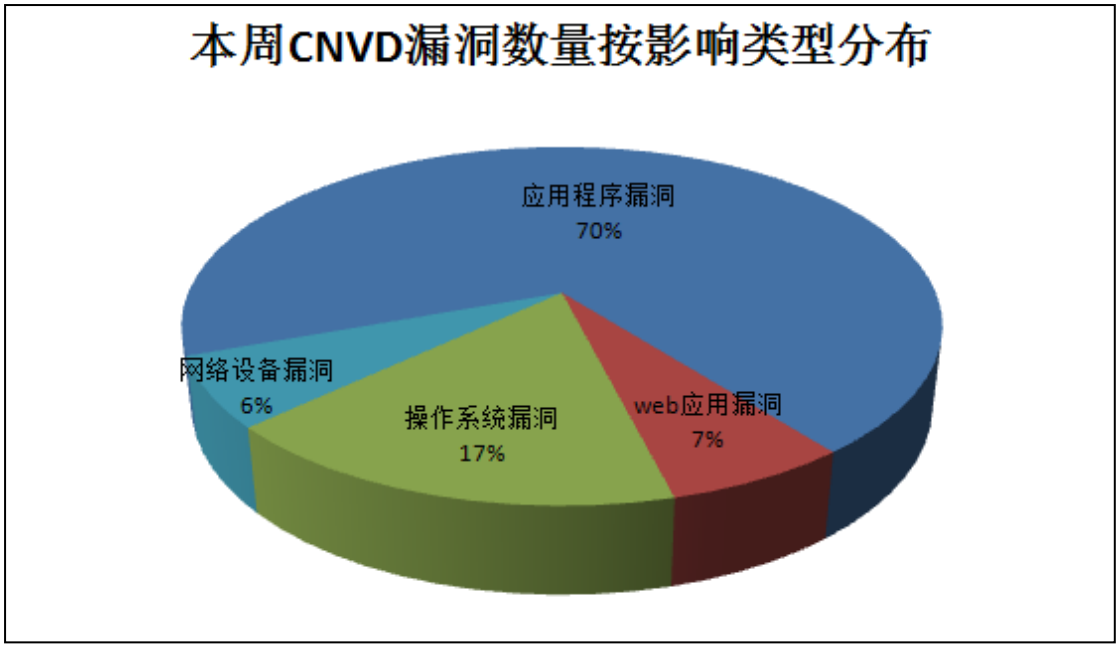

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 21 个电信行业漏洞，196 个移动互联网漏洞，3 个工控行业漏洞（如下图表所示）。其中，“Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CNVD-2014-06425、CNVD-2014-06432、CNVD-2014-06434、CNVD-2014-06437）、Cisco IOS 和 IOS XE Software Multicast DNS Gateway 拒绝服务漏洞、Cisco IOS 和 IOS XE Software Multicast DNS Gateway 内存泄露拒绝服务漏洞、Cisco IOS 和 IOS XE Software DHCPv6 拒绝服务漏洞、Apple iOS IOAcceleratorFamily API 参数拒绝服务漏洞、Apple iOS IntelAccelerator 驱动空指针引用漏洞、Apple iOS Mach ports 两次释放处理任意代码执行漏洞、Apple iOS IOHIDFamily 越界内存读取破坏漏洞、Apple iOS IOHIDFamily 特权提升漏洞、Apple iOS Libnotify 特权提升漏洞、Apple iOS IODataQueue 对象处理任意代码执行漏洞、Apple iOS IOKit 整数溢出漏洞、Apple iOS IOHIDFamily 堆溢出漏洞、Apple iOS IOHIDFamily 空指针引用远程代码执行漏洞、Apple iOS IODataQueue 对象处理任意代码执行漏洞”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-2014-06155	多个 Aztech ADSL2/2+路由器存在多个漏洞	高	否
电信	CNVD-2014-06166	IBM Websphere Message Broker and Integration Bus 信息泄露漏洞	中	是
电信	CNVD-2014-06162	Cisco IOS XR 拒绝服务漏洞	中	是
电信	CNVD-2014-06214	多个 Aztech modem 路由器会话劫持漏洞	中	否
电信	CNVD-2014-06308	Cisco Nexus 1000V InterCloud for Vmware 跨站脚本漏洞	中	否
电信	CNVD-2014-06307	Cisco IOS XR Software RSVP 包解析拒绝服务漏洞	中	是
电信	CNVD-2014-06306	Cisco IOS XR 'snmpd'拒绝服务漏洞	中	是
电信	CNVD-2014-06309	Cisco IOS XR 拒绝服务漏洞（CNVD-2014-06309）	中	是
电信	CNVD-2014-06333	IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2014-06333）	低	是
电信	CNVD-2014-06364	IBM WebSphere Application Server 跨站请求伪造漏洞	中	是
电信	CNVD-2014-06374	Asterisk Open Source SIP SUBSCRIBE 请求拒绝服务漏洞	中	是
电信	CNVD-2014-06373	Asterisk Open Source Out of Call 消息拒绝服务漏洞	中	是
电信	CNVD-2014-06426	ZyXEL P-660HNU-T1 'wzADSL.asp'远程信息泄露漏洞	中	否
电信	CNVD-2014-06425	Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CNVD-2014-06425）	高	是
电信	CNVD-2014-06432	Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CNVD-2014-06432）	高	是
电信	CNVD-2014-06433	Cisco IOS 和 IOS XE Software Multicast DNS Gateway 拒绝服务漏洞	高	是
电信	CNVD-2014-06434	Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CNVD-2014-06434）	高	是
电信	CNVD-2014-06436	Cisco IOS 和 IOS XE Software Multicast DNS Gateway 内存泄露拒绝服务漏洞	高	是
电信	CNVD-2014-06438	Cisco IOS 和 IOS XE Software DHCPv6 拒绝服务漏洞	高	是
电信	CNVD-2014-06437	Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CNVD-2014-06437）	高	是
电信	CNVD-2014-06451	多个 Huawei 交换机信息泄漏漏洞	中	是
移动互联网	CNVD-2014-06122	WebKit 内存破坏漏洞（CNVD-2014-06122）	中	是
移动互联网	CNVD-2014-06123	WebKit 内存破坏漏洞（CNVD-2014-061	中	是

		23）		
移动互联网	CNVD-2014-06124	WebKit 内存破坏漏洞（CNVD-2014-06124）	中	是
移动互联网	CNVD-2014-06125	WebKit 内存破坏漏洞（CNVD-2014-06125）	中	是
移动互联网	CNVD-2014-06126	WebKit 内存破坏漏洞（CNVD-2014-06126）	中	是
移动互联网	CNVD-2014-06127	WebKit 内存破坏漏洞（CNVD-2014-06127）	中	是
移动互联网	CNVD-2014-06128	Apple ios 地址簿读取漏洞	低	是
移动互联网	CNVD-2014-06129	Apple iOS 信息泄露漏洞	中	是
移动互联网	CNVD-2014-06130	Apple iOS/TV 信息泄露漏洞	低	是
移动互联网	CNVD-2014-06131	Facebook Status Via application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06140	Steganos Online Shield VPN application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06139	FastCustomer -- Fast Customer application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06138	DCU Mobile Banking application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06137	10000 Kindle Books Downloads application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06136	Monster Makeup application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06132	ga6748 application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06133	Need for Speed Network application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06134	VK Amberfog application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06135	SurDoc-100GB+FREE storage application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06169	MinhaOi for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06171	Lil Wayne Slots: FREE SLOTS for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06182	Pet Salon for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06183	Kmart @7F0C00EF for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06170	Tigo Copa Mundial FIFA 2014 for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06172	AllDealsAsia All Deals ADA app application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06173	Social Networking application for Andr	中	否

		oid SSL 证书验证漏洞		
移动互联网	CNVD-2014-06174	INCOgnito Private Browser application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06175	Daily Free App @ Amazon application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06176	Flurv Chat application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06177	Coke Studio 7 application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06178	Vodafone Mobile@Work application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06179	Stop & Shop SCAN IT! Mobile application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06180	Store and Share application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06181	emartmall application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06184	Watcha for Android 信息泄露漏洞	中	是
移动互联网	CNVD-2014-06198	Apple iOS 蓝牙自启动漏洞	中	是
移动互联网	CNVD-2014-06199	Apple iOS 安全绕过短消息信息泄露漏洞	低	是
移动互联网	CNVD-2014-06185	Soccer Blitz application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06186	LabMSF Antivirus beta application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06187	Baby Stomach Surgery application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06188	Armpit Spa & Girl Games application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06189	PocketPC.ch application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06190	travelzadcomvb application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06200	Apple iOS 前端 App 判断漏洞	中	是
移动互联网	CNVD-2014-06201	Apple iOS 沙盒绕过 Apple ID 信息泄露漏洞	中	是
移动互联网	CNVD-2014-06202	Apple iOS 启动填充敏感信息泄露漏洞	中	是
移动互联网	CNVD-2014-06203	Apple iOS 敏感信息泄露漏洞	中	是
移动互联网	CNVD-2014-06204	Apple iOS LOGINDISABLED IMAP 信息泄露漏洞	中	是
移动互联网	CNVD-2014-06205	Apple iOS 升级语音拨号设置漏洞	低	是
移动互联网	CNVD-2014-06206	Apple iOS AssistiveTouch 设置错误漏洞	中	是

移动互联网	CNVD-2014-06207	Apple iOS IOAcceleratorFamily API 参数拒绝服务漏洞	高	是
移动互联网	CNVD-2014-06208	Apple iOS 敏感内存信息泄露漏洞	低	是
移动互联网	CNVD-2014-06209	Apple iOS 任意文件权限更改漏洞	低	是
移动互联网	CNVD-2014-06210	Apple iOS IntelAccelerator 驱动空指针引用漏洞	高	是
移动互联网	CNVD-2014-06211	Apple iOS XML 外部实体信息泄露漏洞	中	是
移动互联网	CNVD-2014-06212	Apple iOS Mach ports 两次释放处理任意代码执行漏洞	高	是
移动互联网	CNVD-2014-06213	Apple iOS PDF 文件整数溢出漏洞	中	是
移动互联网	CNVD-2014-06215	Apple iOS PDF 文件越界读漏洞	中	是
移动互联网	CNVD-2014-06216	Apple iOS IOHIDFamily 越界读漏洞	高	是
移动互联网	CNVD-2014-06217	Apple iOS IOHIDFamily 特权提升漏洞	高	是
移动互联网	CNVD-2014-06218	Apple iOS Libnotify 特权提升漏洞	高	是
移动互联网	CNVD-2014-06219	Apple iOS 升级失败漏洞	中	是
移动互联网	CNVD-2014-06220	Apple iOS 未校验应用安装漏洞（CNVD-2014-06220）	低	是
移动互联网	CNVD-2014-06221	Apple iOS 未校验应用安装漏洞	低	是
移动互联网	CNVD-2014-06222	Apple iOS IODataQueue 对象处理任意代码执行漏洞	高	是
移动互联网	CNVD-2014-06223	Apple iOS IOKit 整数溢出漏洞	高	是
移动互联网	CNVD-2014-06224	Apple iOS IOHIDFamily 堆溢出漏洞	高	是
移动互联网	CNVD-2014-06225	Apple iOS IOHIDFamily 空指针引用远程代码执行漏洞	高	是
移动互联网	CNVD-2014-06226	Apple iOS IOKit 内存泄露漏洞	中	是
移动互联网	CNVD-2014-06227	Apple iOS rt_setgate()越界读漏洞	中	是
移动互联网	CNVD-2014-06228	Apple iOS 缓存数据处理敏感信息泄露漏洞	中	是
移动互联网	CNVD-2014-06229	Apple iOS IODataQueue 对象处理任意代码执行漏洞	高	是
移动互联网	CNVD-2014-06230	Apple iOS 敏感内存信息泄露漏洞（CNVD-2014-06230）	低	是
移动互联网	CNVD-2014-06231	Apple iOS 敏感内存信息泄露漏洞（CNVD-2014-06231）	低	是
移动互联网	CNVD-2014-06232	Apple iOS 敏感内存信息泄露漏洞（CNVD-2014-06232）	低	是
移动互联网	CNVD-2014-06239	Apple iOS 随机数生成器安全绕过漏洞	中	是
移动互联网	CNVD-2014-06238	Apple iOS 沙盒绕过信息泄露漏洞	中	是
移动互联网	CNVD-2014-06241	Mzone Login application for Android SSL 证书验证漏洞	高	否
移动互联网	CNVD-2014-06251	Harley-Davidson Visa application for Android SSL 证书验证漏洞	中	否

移动互联网	CNVD-2014-06252	Versent Books application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06249	s-peek credit rating report application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06250	LG Telepresence application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06247	Facebook Facts application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06248	wTMDesktop application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06246	TIO MobilePay - Bill Payments application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06244	DNB Trade application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06245	Homesteading Today application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06243	Mark's Daily Apple Forum application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06242	FIAT Forum application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06269	Alien War Survivors for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06270	VPlayer Video Player for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06271	Atomic Fusion for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06272	State Bank Anywhere for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06263	Microsoft Mobile Nokia Asha 501 安全绕过漏洞	中	是
移动互联网	CNVD-2014-06254	Pocket Cam Photo Editor for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06253	Fuel Rewards Network application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06273	KASKUS for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06274	E-Dziennik for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06275	SinoPac for Android 信息泄露漏洞	中	是
移动互联网	CNVD-2014-06277	NOW for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06276	TICKET APP - Concerts & Sports for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06278	Obama for America for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06282	psicofxp for Android 信息泄露漏洞	中	否

移动互联网	CNVD-2014-06283	forumhawaaworldcom for Android 信息泄露漏洞	中	是
移动互联网	CNVD-2014-06284	Edline Mobile for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06286	Conquest Of Fantasia application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06281	Celluloid application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06285	Doodle Drop application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06280	global beauty research application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06279	psychology application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06296	Survey.com Mobile application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06295	Gratta& Vinci? application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06294	LikeHero Get Instagram Likes application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06293	Blitz Bingo application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06292	Zombie Detector application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06291	Rasta Weed Widgets HD application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06290	cutprice application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06289	Gravity Bounce application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06288	nuSquare application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06287	TuCarro application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06311	Loving - Couple Essential for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06312	Aquarium Advice for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06313	PSECU Mobile+ for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06305	memetan for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06303	baby days for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06301	cookbible for Android 信息泄露漏洞	中	否

移动互联网	CNVD-2014-06314	RunKeeper - GPS Track Run Walk application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06310	Threadflip : Buy, Sell Fashion application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06304	Little Dragons application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06302	gewara application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06315	eponyms for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06316	Alibaba for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06317	Mobile Face for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06319	TV Bengali Open Directory for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06320	Azkend Gold for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06321	Bump for Android 信息泄露漏洞	中	是
移动互联网	CNVD-2014-06322	My3 - by 3HK for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06323	Educational Puzzles - Letters for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06324	Animal Kaiser Zangetsu for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06318	Fiksu library for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06336	MLB Preplay for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06337	DEKRA Used Car Report for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06338	Auto Trader for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06339	SkyDrive Assistant for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06340	autonavi for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06334	DTE Energy for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06335	BelasFrases de Amor for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06342	Skin Conditions and Diseases for Android SSL 信息泄露漏洞	中	否

移动互联网	CNVD-2014-06344	cekpetblycnexa for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06341	FreshDirect for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06346	ding* ezetop. Top-up Any Phone for Android 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06386	MOL bringaPONT for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06383	Open Electrical Webser for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06382	Mahabharata Audiocast for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06381	davidheysuperheroquiz for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06380	EPISD Parent Portal for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06379	Exercitiipentru abdomen for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06377	MyFitnessPal for Android 信息泄露漏洞	中	是
移动互联网	CNVD-2014-06401	Yuko Yukofor Android SSL 信息泄露漏洞	中	是
移动互联网	CNVD-2014-06394	JW Cards for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06393	Voices.com for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06391	Zoho Books - Accounting App for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06390	Tsushima Travel Guide for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06397	Algeria Radio for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06396	Ticket Round Up for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06400	Ruta Exacta for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06399	World Cup 2014 Brazil - Xem TV application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06395	African Radios Live application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06408	Addis Gag Funny Amharic Pic application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06403	Forum Krstarice application for Android SSL 证书验证漏洞	中	否

移动互联网	CNVD-2014-06402	netease movie application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06398	bellyhoodcom application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06415	Inside Crochet application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06414	racemotocross application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06413	Baglamukhi application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06412	Ahmed BukhatirNasheeds TV application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06411	Latin Angels Music HD application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06421	Leadership Newspapers application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06420	drareym application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06419	Tortoise Forum application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06418	wTrootrooTvIzle application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06417	Afghan Radio application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06416	Planet of the Vapes Forum application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06428	Smart Browser application for Android SSL 证书验证漏洞	中	是
移动互联网	CNVD-2014-06431	eWUŚ mobile for Android SSL 信息泄露漏洞	中	否
移动互联网	CNVD-2014-06427	Batch library for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06430	SingaporeMotherhood Forum for Android 信息泄露漏洞	中	是
移动互联网	CNVD-2014-06424	KoleksiHadisNabi SAW application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06423	Defence.pk application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06422	Apploi Job Search- Find Jobs application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06450	NextGenUpdate application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06449	iPhone4.TW application for Android SSL 证书验证漏洞	中	否

移动互联网	CNVD-2014-06448	ElForro.com application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06442	SLFileManager for Android 目录遍历漏洞	中	否
移动互联网	CNVD-2014-06456	Wizaz Forum application for Android SSL 证书验证漏洞	中	否
移动互联网	CNVD-2014-06457	MyBroadbandTapatalk application for Android SSL 证书验证漏洞	中	否
工控系统	CNVD-2014-06121	Schneider Electric ClearSCADA 存在远程未明漏洞	中	是
工控系统	CNVD-2014-06196	Schneider Electric ClearSCADA 跨站脚本漏洞	低	是
工控系统	CNVD-2014-06447	WS10 Data Server SCADA 缓冲区溢出漏洞	中	否

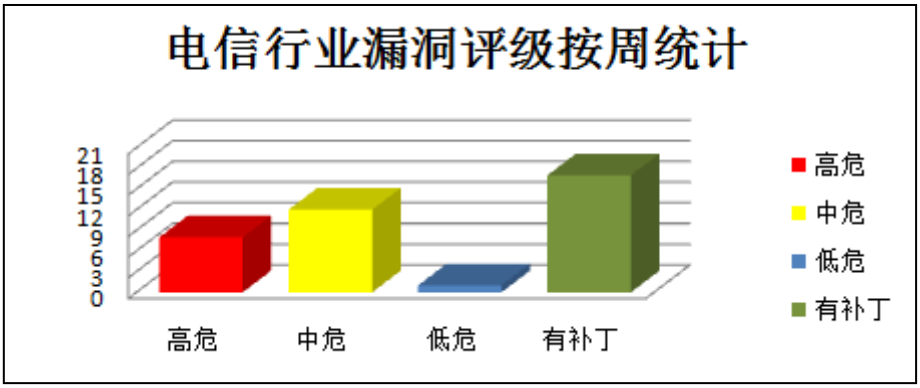

图 1 电信行业漏洞统计

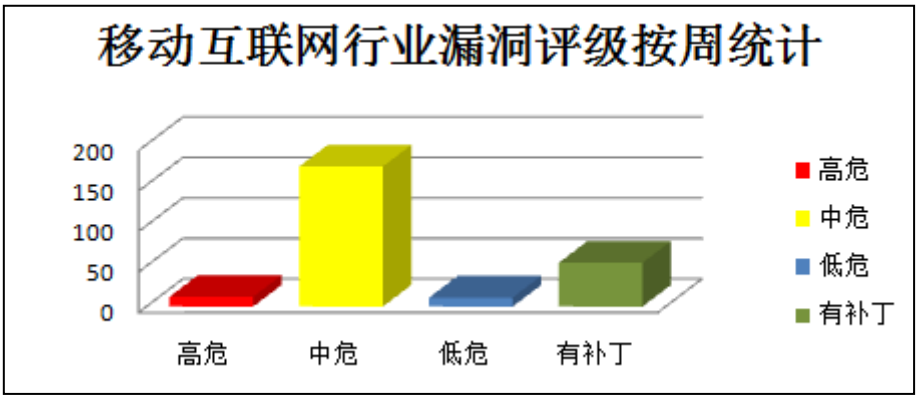

图 2 移动互联网行业漏洞统计

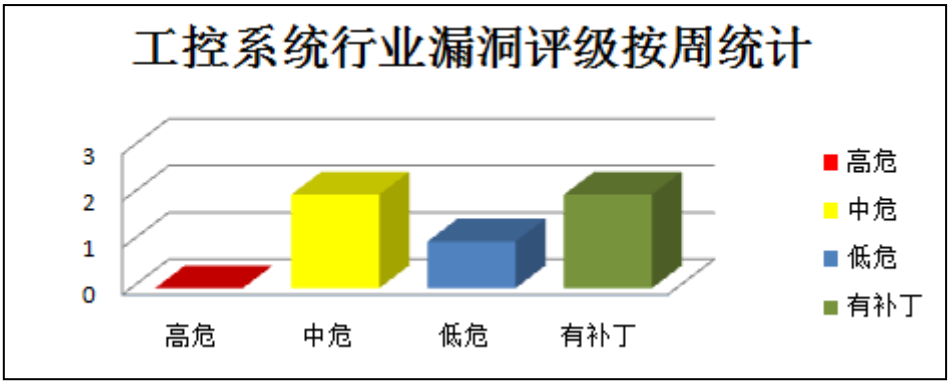

图 3 工控系统行业漏洞统计

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、 GNU 产品安全漏洞

9 月 25 日，CNVD 收录了 GNU Bash 远程代码执行漏洞（CNVD-2014-06345，对应 CVE-2014-6271），官方同步提供了 GNU Bash 的修复补丁。9 月 25 日晚，安全人员研究发现其提供的补丁程序并未完全修复漏洞，相关安全机制可被绕过，对互联网上应用 GNU Bash 的大量服务器构成远程控制威胁。

CNVD 收录的相关漏洞包括：GNU Bash 远程代码执行漏洞、GNU Bash 不完整修复远程代码执行漏洞。上述漏洞的综合评级均为“高危”。其中“GNU Bash 远程代码执行漏洞”厂商已经发布了修补程序。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-2014-06435

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06345

2、 Apple 产品安全漏洞

Apple Mac OS X Server 是美国苹果（Apple）公司的一套服务器操作系统；Apple iOS 是一款运行在苹果 iPhone 和 iPod touch 设备上的最新的操作系统。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息或以系统权限执行任意代码。

CNVD 收录的相关漏洞包括：Apple Mac OS X Server SQL 注入漏洞、Apple Mac OS X 任意代码执行漏洞（CNVD-2014-06159）、Apple OS X Bluetooth API 调用任意代码执行漏洞、Apple OS X GLSL shaders 编译缓冲区溢出漏洞、Apple OS X IOKit API 参数空指针应用任意代码执行漏洞、Apple iOS IODataQueue 对象处理任意代码执行漏洞、Apple iOS IOHIDFamily 空指针引用远程代码执行漏洞、Apple iOS IOHID

Family 堆溢出漏洞。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-2014-06158

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06159

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06234

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06233

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06235

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06229

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06225

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06224

3、IBM 产品安全漏洞

IBM QRadar 通过监控及关联日志和流量来识别这种异常行为；QRadar SIEM 可以把散布于整个网路上、数以千计的装置端点与应用程式中的日志来源事件资料加以合并；IBM Rational ClearCase 是软件配置管理(SCM)工具；IBM WebSphere Message Broker（现称 IBM Integration Bus）是美国 IBM 公司的一款企业服务总线（ESB）产品；IBM WebSphere Application Server（WAS）是美国 IBM 公司开发并发行的一款应用服务器产品，它是 Java EE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。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、发起拒绝服务或进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：IBM QRadar Security Information and Event Manager 远程代码执行漏洞、IBM Rational ClearCase XML 实体扩展拒绝服务漏洞、IBM WebSphere Application Server 跨站请求伪造漏洞、IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2014-06333）、IBM Rational ClearQuest 验证绕过漏洞、IBM Rational ClearQuest 信息泄露漏洞（CNVD-2014-06258）、IBM Rational ClearQuest 安全绕过漏洞、IBM Websphere Message Broker and Integration Bus 信息泄露漏洞。其中“IBM QRadar Security Information and Event Manager 远程代码执行漏洞”的综合评级为“高危”。目前，厂商已经发布了修补程序。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-2014-06358

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06362

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06364

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06333

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06257

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06258

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06259

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06166

4、Cisco 产品安全漏洞

Cisco IOS 是多数思科系统路由器和网络交换机上使用的互联网络操作系统；Cisco Unified Communications Manager 是一款 Cisco IP 电话解决方案中的呼叫处理组件；Cisco Nexus 1000V InterCloud for VMware 是美国思科（Cisco）公司的一套虚拟交换机软件。本周，上述产品被披露存在拒绝服务和跨站脚本漏洞，攻击者可利用漏洞发起拒绝服务和跨站脚本攻击。

CNVD 收录的相关漏洞包括：Cisco Unified Communications Domain Manager 远程拒绝服务漏洞、Cisco IOS XR 拒绝服务漏洞、Cisco IOS XR 拒绝服务漏洞（CNVD-2014-06309）、Cisco IOS XR 'snmpd'拒绝服务漏洞、Cisco IOS XR Software RSVP 包解析拒绝服务漏洞、Cisco Nexus 1000V InterCloud for Vmware 跨站脚本漏洞、Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CNVD-2014-06437、CNVD-2014-06432）。其中“Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CNVD-2014-06437、CNVD-2014-06432）”的综合评级为“高危”。其中，除“Cisco Unified Communications Domain Manager 远程拒绝服务漏洞、Cisco Nexus 1000V InterCloud for Vmware 跨站脚本漏洞”外，厂商已经发布了其余漏洞的修补程序。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-2014-06299

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06162

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06309

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06306

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06307

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06308

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06437

http://www.cnvd.org.cn/flaw/show/CNVD-2014-06432

5、Zend Framework Sqlsrv Driver 存在多个 SQL 注入漏洞

Zend Framework (ZF)是一个开放源代码的 PHP5 开发框架，可用于来开发 web 程序和服务。本周，Zend Framework (ZF)被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可利用漏洞注入任意 SQL 代码，操作数据库。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-2014-06376

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-2014-06155	多个 Aztech ADSL2/2+路由器存在多个漏洞	高	暂无
CNVD-2014-06192	Junos Pulse Secure Access Service/Junos Pulse Client 特权提升漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞：http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10644&cat=SIRT_1&actp=LIST
CNVD-2014-06241	Mzone Login application for Android SSL 证书验证漏洞	高	暂无
CNVD-2014-06361	Symfony Web Profiler 跨站请求伪造漏洞	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://symfony.com/
CNVD-2014-06356	Node.js syntax-error module 'eval()'函数任意代码执行漏洞	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://nodejs.org/
CNVD-2014-06371	LibVNCServer 存在多个缓冲区溢出漏洞	高	用户可以联系供应商获得补丁信息：http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6055
CNVD-2014-06368	LibVNCServer 整数溢出漏洞	高	用户可以联系供应商获得补丁信息：http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6051
CNVD-2014-06407	X2CRM 'FileUploadsFilter.php'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.x2engine.com/
CNVD-2014-06410	Debian 'apt' Package 缓冲区溢出漏洞	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.debian.org/
CNVD-2014-06445	WordPress 插件 WP file upload 和 manager by N-Media 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：https://wordpress.org/plugins

表 3 部分高危漏洞列表

小结：本周，移动互联网行业漏洞数增多，主要原因是 Apple iOS 存在多个漏洞及许多 Android 应用程序存在 SSL 证书验证漏洞，允许攻击者利用漏洞获取敏感信息，执行任意代码，提升权限，发起中间人或拒绝服务攻击，请各应用软件方注意防范 Apple iOS 漏洞及 Android SSL 证书验证绕过漏洞。值得注意的是，GNU 被披露存在远程代

码执行和不完整修复远程代码执行漏洞，攻击者可利用漏洞在应用程序上下文中执行任意代码。此外，Apple、IBM、Cisco 多款产品被披露存在多个漏洞，攻击者利用漏洞可获取敏感信息，执行任意脚本或跨站代码，发起拒绝服务攻击。另外，Zend Framework 被披露存在一个高危零日漏洞。攻击者可利用漏洞注入任意 SQL 代码，查看或者修改数据库信息。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、Linux 修补 Kernel 产品漏洞

Linux Kernel 是 Linux 操作系统的内核。

本周，Linux 修补了上述产品存在拒绝服务漏洞，避免攻击者利用漏洞使内核崩溃，导致拒绝服务。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/50235

本周要闻速递

1. GNU Bash 存在远程代码执行漏洞

BASH 除了可以将 shell 变量导出为环境变量，还可以将 shell 函数导出为环境变量！当前版本的 bash 通过以函数名作为环境变量名，以“（）{”开头的字串作为环境变量的值来将函数定义导出为环境变量。最近，BASH 爆出来一个远程代码执行的漏洞。此漏洞爆出在于 BASH 处理这样的“函数环境变量”的时候，并没有以函数结尾“}”为结束，而是一直执行其后的 shell 命令！目前，接受 HTTP 命令的 CGI Shell 脚本是最主要的被攻击对象。此外，OpenSSH 也因其 AcceptEnv、TERM、SSH_ORIGINAL_COMMAND 等环境变量受此漏洞影响。

参考链接：http://www.freebuf.com/news/44768.html

2. GNU Bash 漏洞初步补丁并不完整

在 AusCERT（澳大利亚计算机应急响应小组）公布 Bash 的漏洞利用后，修补该 0 day 已经刻不容缓。大多数 Linux 发行版本的漏洞补丁已发布，但是红帽公司却发布了一个公告警示，该补丁打得并不完全，更改环境变量可能会导致任意代码执行。由此产生的新漏洞编号为 CVE-2014-7169，其中详细阐释了这个情况。红帽公司表示它会发布一个新的补丁。

参考链接：http://www.freebuf.com/news/44948.html

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