

信息安全漏洞周报

2013 年 09 月 23 日-2013 年 09 月 29 日

2013 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 227 个，其中高危漏洞 67 个、中危漏洞 141 个、低危漏洞 19 个。上述漏洞中，可利用来实施远程攻击的漏洞有 198 个。本周收录的漏洞中，已有 185 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“WordPress NoSpamPTI Plugin ‘comment_post_ID’参数 SQL 注入漏洞”、“Real Estate PHP Scrip listingid 参数 SQL 注入漏洞”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 家成员单位及个人报送了本周收录的全部 227 个漏洞。各单位报送情况如表 1 所示。其中，安天实验室、启明星辰、天融信、绿盟科技等单位报送数量较多。此外，个人报送者向 CNVD 提交了 4 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
安天实验室	182	0
启明星辰	154	0
天融信	69	0
绿盟科技	60	0
恒安嘉新	21	0
东软	3	0
个人	4	4

报送总计	493	4
录入总计	227（去重）	4

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、Cisco、FFmpeg 、IBM、WordPress 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	43	20%
2	Cisco	34	15%
3	FFmpeg	14	6%
4	IBM	14	6%
5	WordPress	12	5%
6	TYPO3	8	4%
7	Wireshark	8	4%
8	Hp	8	4%
9	Open-Xchange	4	2%
10	X.Org	4	2%
11	其它	78	32%

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 227 个漏洞。其中应用程序漏洞 140 个，WEB 应用漏洞 35 个，操作系统漏洞 28 个，网络设备漏洞 22 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	140
WEB 应用漏洞	35
网络设备漏洞	22
操作系统漏洞	28
安全产品漏洞	2
数据库漏洞	0

表 3 漏洞按影响类型统计表

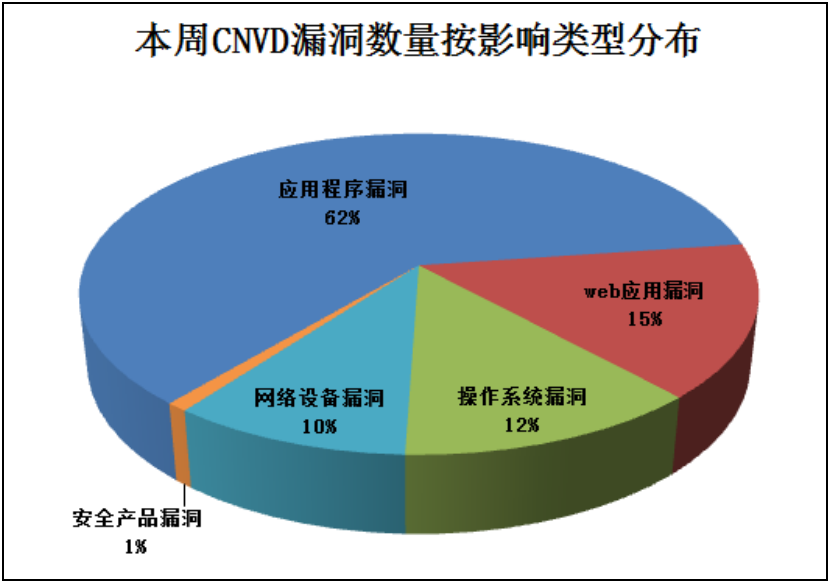


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 21 个电信行业漏洞、46 个移动互联网漏洞和 6 个工控系统行业漏洞（如下列表所示）。其中，20 个漏洞的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。本周，CNVD 未收录移动互联网行业漏洞。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-13384	Cisco IOS XR Software CGSE 和 ISM 远程拒绝服务漏洞	中	是
电信	CNVD-2013-13386	SEIL 多个产品 RADIUS 验证随机数生成漏洞	中	是
电信	CNVD-2013-13388	D-Link DSL-2740B 路由器跨站请求伪造漏洞	低	否
电信	CNVD-2013-13326	Cisco IOS/IOS XE RSVP 接口队列插入远程拒绝服务漏洞	高	是
电信	CNVD-2013-13327	Cisco IOS NAT 功能 PPTP 报文处理远程拒绝服务漏洞	高	是
电信	CNVD-2013-13329	Cisco IOS 网络地址转换远程拒绝服务漏洞（CNVD-2013-13329）	高	是
电信	CNVD-2013-13328	Cisco IOS 网络地址转换远程拒绝服务漏洞（CNVD-2013-13328）	高	是
电信	CNVD-2013-13331	Cisco IOS 域防火墙和内容过滤远程拒绝服务漏洞	高	是
电信	CNVD-2013-13330	Cisco IOS 队列插入远程拒绝	高	是

		服务漏洞		
电信	CNVD-2013-13332	Cisco IOS IPv6 虚拟分片重组 远程拒绝服务漏洞	高	是
电信	CNVD-2013-13333	Cisco IOS/IOS XE Internet 密 钥交换处理远程拒绝服务漏 洞	高	是
电信	CNVD-2013-13334	Cisco IOS 组播网络时间协议 远程拒绝服务漏洞	高	是
电信	CNVD-2013-13230	SEIL 系列路由器 PPPAC L2TP 消息处理缓冲区溢出漏洞	高	是
电信	CNVD-2013-13350	Motorola Defy XT - Republic Wireless 本地权限提升漏洞	中	否
电信	CNVD-2013-13354	Motorola Defy XT - Republic Wireless 栈缓冲区溢出漏洞	中	否
电信	CNVD-2013-13228	D-Link Japan DWL-2100AP SSH 实现登录访问拒绝服务漏 洞	中	是
电信	CNVD-2013-13232	Cisco Unified Computing System 光纤互连字符串处理 远程溢出漏洞	中	是
电信	CNVD-2013-13233	Cisco AnyConnect Secure Mobility 客户端本地权限提升 漏洞	中	是
电信	CNVD-2013-13206	IBM WebSphere Application Server 跨站脚本漏洞 (CNVD-2013-13206)	中	是
电信	CNVD-2013-13207	IBM WebSphere Application Server 跨站脚本漏洞 (CNVD-2013-13207)	中	是
电信	CNVD-2013-13208	IBM WebSphere Application Server 权限控制漏洞	中	是
移动互联 网	CNVD-2013-13350	Motorola Defy XT - Republic Wireless 本地权限提升漏洞	中	否
移动互联 网	CNVD-2013-13354	Motorola Defy XT - Republic Wireless 栈缓冲区溢出漏洞	中	否
移动互联 网	CNVD-2013-13317	Share KM 远程拒绝服务漏洞	高	否
移动互联 网	CNVD-2013-13263	ShareKM 远程拒绝服务漏洞	中	否
移动互联 网	CNVD-2013-13286	Apple iPhone 5s TouchID 指纹 重放验证绕过漏洞	中	否
移动互联 网	CNVD-2013-13287	Apple iOS SIRI 个人语音助手 验证绕过漏洞	中	否
移动互联	CNVD-2013-13289	Android FTP Server 任意文件	高	否

网		访问漏洞		
移动互联 网	CNVD-2013-13242	Apple iOS TrustWave 作废 sub-CA 证书 TLS 中间人攻击 漏洞	中	是
移动互联 网	CNVD-2013-13180	Apple iPhone/iPad/iPod touch iOS 拒绝服务漏洞	中	是
移动互联 网	CNVD-2013-13181	Apple iPhone/iPad/iPod touch iOS 沙箱绕过漏洞	中	是
移动互联 网	CNVD-2013-13183	Apple iPhone/iPad/iPod touch iOS 内存破坏漏洞	中	是
移动互联 网	CNVD-2013-13184	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13184）	中	是
移动互联 网	CNVD-2013-13185	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13185）	中	是
移动互联 网	CNVD-2013-13187	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13187）	中	是
移动互联 网	CNVD-2013-13186	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13186）	中	是
移动互联 网	CNVD-2013-13189	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13189）	中	是
移动互联 网	CNVD-2013-13188	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13188）	中	是
移动互联 网	CNVD-2013-13191	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13191）	中	是
移动互联 网	CNVD-2013-13190	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13190）	中	是
移动互联 网	CNVD-2013-13193	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13193）	中	是
移动互联 网	CNVD-2013-13192	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13192）	中	是
移动互联 网	CNVD-2013-13194	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13194）	中	是
移动互联 网	CNVD-2013-13195	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13195）	中	是
移动互联 网	CNVD-2013-13196	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13196）	中	是
移动互联 网	CNVD-2013-13198	WebKit 存在未明内存破坏漏 洞（CNVD-2013-13198）	中	是
移动互联 网	CNVD-2013-13199	Apple iPhone/iPad/iPod touch 存在多个跨站脚本漏洞	中	是
移动互联 网	CNVD-2013-13201	Apple iOS IOKit 后台 App 用户 接口事件注入漏洞	低	是
移动互联 网	CNVD-2013-13200	Apple iPhone/iPad/iPod touch 跨站脚本漏洞	中	是

移动互联网	CNVD-2013-13204	Apple iOS 内核畸形报文处理 远程拒绝服务漏洞	高	是
移动互联网	CNVD-2013-13203	Apple iOS IOSerialFamily 越界 数组访问任意本地代码执行 漏洞	高	是
移动互联网	CNVD-2013-13202	Apple iOS IOKitUser IOCatalogue 空指针引用本地 拒绝服务漏洞	低	是
移动互联网	CNVD-2013-13211	Apple iOS 内核 msgctl / segctl API 本地内核内存泄露漏洞	中	是
移动互联网	CNVD-2013-13205	Apple iOS 内核套接字接口整 数截断拒绝服务漏洞	高	是
移动互联网	CNVD-2013-13215	Apple iOS 未授权推送通知令 牌泄露漏洞	中	是
移动互联网	CNVD-2013-13214	Apple iOS SIM 卡弹出竞争条 件锁屏绕过漏洞	中	是
移动互联网	CNVD-2013-13213	Apple iOS Kext Management 特制 IPC 消息加载内核扩展操 作漏洞	低	是
移动互联网	CNVD-2013-13217	Apple iOS Safari 明文 Content-Type 处理跨站脚本漏 洞	中	是
移动互联网	CNVD-2013-13216	Apple iOS Safari 历史记录处 理敏感信息泄露漏洞	低	是
移动互联网	CNVD-2013-13218	Apple iOS Safari 存在未明 URL 栏伪造漏洞	中	是
移动互联网	CNVD-2013-13219	Apple iOS Springboard lost 模 式通知内容泄露漏洞	低	是
移动互联网	CNVD-2013-13221	Apple iOS 第三方 App /dev/random 拒绝服务漏洞	高	是
移动互联网	CNVD-2013-13220	Apple iOS 第三方 App 脚本识 别沙盒绕过漏洞	中	是
移动互联网	CNVD-2013-13224	Apple iOS Twitter 账户交互本 地信息泄露漏洞	低	是
移动互联网	CNVD-2013-13223	Apple iOS Twitter 子系统后台 请求安全绕过漏洞	中	是
移动互联网	CNVD-2013-13222	Apple iOS 电话功能访问控制 绕过漏洞	中	是
移动互联网	CNVD-2013-13225	Apple iPhone/iPad/iPod touch iOS 信息泄露漏洞 (CNVD-2013-13225)	中	是
工控系统	CNVD-2013-13325	ClearSCADA Web 请求处理远 程拒绝服务漏洞	中	是
工控系统	CNVD-2013-13371	Invensys Wonderware InTouch	中	是

		XML 外部实体敏感信息泄漏漏洞		
工控系统	CNVD-2013-13375	多个 Emerson Process Management RTUs 内置账户安全绕过漏洞	高	是
工控系统	CNVD-2013-13376	多个 Emerson Process Management RTUs 远程漏洞	高	是
工控系统	CNVD-2013-13377	Emerson ROC800 远程终端单元远程代码执行漏洞	高	是
工控系统	CNVD-2013-13378	多个 Emerson Process Management RTUs 任意文件上传漏洞	高	是

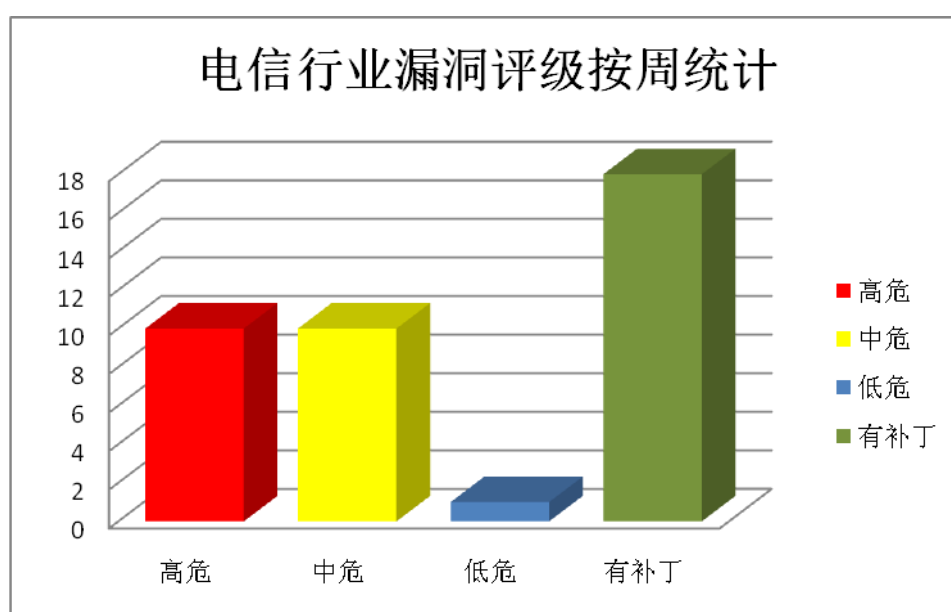


图 2 电信行业漏洞统计

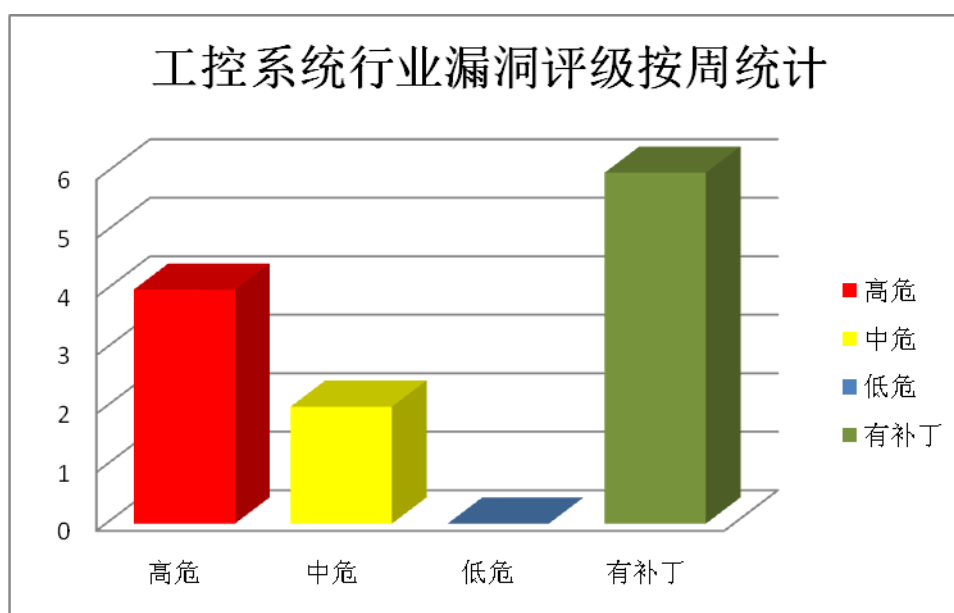


图 3 工控系统行业漏洞统计

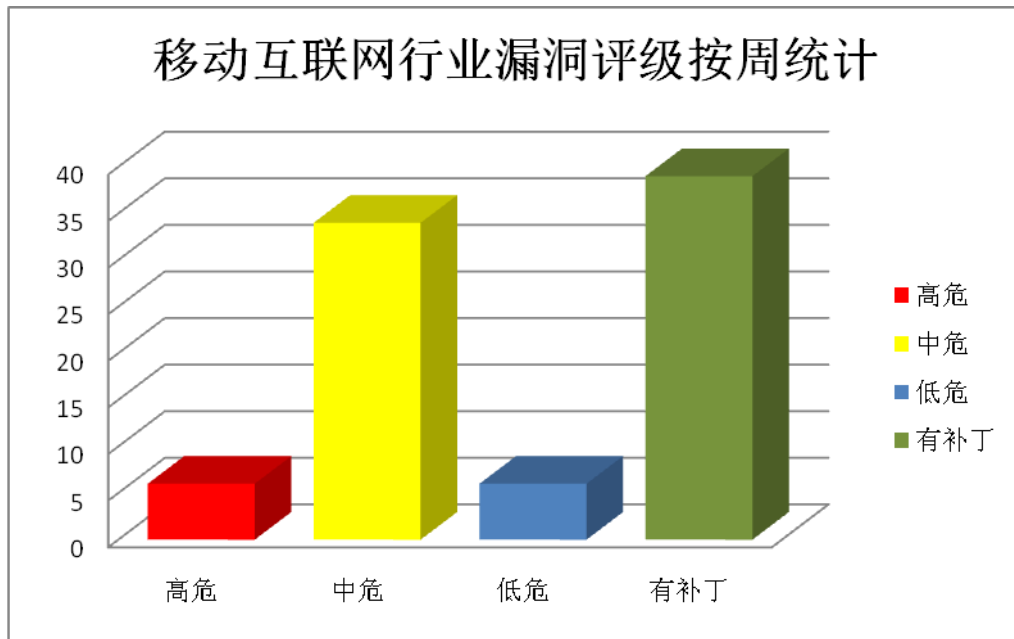


图 3 移动互联网行业漏洞统计

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、Apple 产品安全漏洞

Apple iTunes 是一款媒体播放程序；Apple iOS 是运行在苹果 iPhone 和 iPod touch 设备上的操作系统。本周，上述产品被披露存在多个安全漏洞。利用上述漏洞，攻击者可执行任意代码或发起拒绝服务攻击，获取内核栈内存信息。

CNVD 收录的相关漏洞包括：Apple iTunes ActiveX 内存破坏漏洞、Apple iOS 内核畸形报文处理远程拒绝服务漏、Apple iPhone/iPad/iPod touch iOS 内存破坏漏洞、Apple iOS IOSerialFamily 越界数组访问任意本地代码执行漏洞、Apple iOS 内核套接字接口整数截断拒绝服务漏洞、Apple iOS 第三方 App /dev/random 拒绝服务漏洞、Apple iOS 内核 msgctl / segctl API 本地内核内存泄露漏洞、Apple iPhone/iPad/iPod touch iOS 拒绝服务漏洞。其中，除“Apple iPhone/iPad/iPod touch iOS 内存破坏漏洞、Apple iOS 内核 msgctl / segctl API 本地内核内存泄露漏洞、Apple iPhone/iPad/iPod touch iOS 拒绝服务漏洞”外，其余漏洞的综合评级均为“高危”。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-2013-13182>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13204>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13203>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13205>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13221>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13183>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13211>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13180>

2、WordPress 插件安全漏洞

WordPress 基于 PHP 的博客平台，用户可以在支持 PHP 和 MySQL 数据库的服务器上架设自己的网志。本周，WordPress 的多款插件被披露存在多个安全漏洞，攻击者利用漏洞可获取敏感信息或劫持用户会话，上传和执行任意 PHP 文件，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：WordPress mb.miniAudioPlayer 插件跨站脚本漏洞、WordPress 插件 Platinum SEO 跨站脚本漏洞、WordPress 插件 WP Ultimate Email Marketer 安全绕过漏洞、WordPress 插件 Custom Website Data 'ref'参数跨站脚本漏洞、Wordpress Lazy SEO 插件 Shell 上传漏洞、WordPress NOSpamPTI Plugin 'comment_post_ID'参数 SQL 注入漏洞、WordPress 插件 TimThumb 存在多个漏洞、RocketTheme 多个 WordPress 插件 TimThumb 存在多个漏洞。其中“WordPress 插件 WP Ultimate Email Marketer 安全绕过漏洞、Wordpress Lazy SEO 插件 Shell 上传漏洞、WordPress NOSpamPTI Plugin 'comment_post_ID'参数 SQL 注入漏洞”的综合评级均为“高危”。厂商已经发布了“RocketTheme 多个 WordPress 插件 TimThumb 存在多个漏洞、WordPress 插件 TimThumb 存在多个漏洞、WordPress 插件 Platinum SEO 跨站脚本漏洞”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安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13321>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13342>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13308>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13309>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13316>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13291>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13293>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13292>

3、Cisco 产品安全漏洞

Cisco IOS 是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 Computing System 是一个集计算、虚拟化和网络于一体的平台；Cisco Prime Data Center Network Manager 也称为 Cisco Data Center Network Manager，是一款网络管理应用程序；Cisco Prime 是一款以服务为中心的解决方案。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞可发起拒绝服务攻击，获取敏感信息，执行任意命令。

CNVD 收录的相关漏洞包括：Cisco IOS NAT 功能 PPTP 报文处理远程拒绝服务漏洞、Cisco IOS/IOS XE RSVP 接口队列插入远程拒绝服务漏洞、Cisco IOS 网络地址转换远程拒绝服务漏洞（CNVD-2013-13328）、Cisco IOS 域防火墙和内容过滤远程拒绝服务漏洞、Cisco IOS 队列插入远程拒绝服务漏洞、Cisco IOS/IOS XE Internet 密钥交换处理远程拒绝服务漏洞、Cisco Prime Data Center Network Manager SAN 服务器组件任意文件泄漏洞、Cisco Prime Central for Hosted Collaboration Solution Assurance 信息泄露。上述漏洞的综合评级均为“高危”。厂商已经发布了这些漏洞的修补程序。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-2013-13327>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13326>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13328>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13331>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13330>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13333>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13244>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13238>

4、IBM 产品安全漏洞

IBM Analytical Decision Management 是一款预测分析软件；IBM iNotes 是一个 Web 解决方案；WebSphere 是 IBM 的集成软件平台；Rational ClearCase 是一款软件配置管理（SCM）工具。本周，上述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，执行任意代码。

CNVD 收录的相关漏洞包括：IBM Rational ClearCase 本地权限提升漏洞、IBM Analytical Decision Management 存在未明跨站脚本漏洞、IBM Analytical Decision Management 存在未明远程代码执行漏洞、IBM Analytical Decision Management 存在未明任意文件上传漏洞、IBM iNotes 存在未明缓冲区溢出漏洞、IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2013-13206）、IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2013-13207）、IBM WebSphere Application Server 权限控制漏洞。其中“IBM Analytical Decision Management 存在未明远程代码执行漏洞、IBM iNotes 存在未明缓冲区溢出漏洞”的综合评级均为“高危”。厂商已发布了上述漏洞的修补程序。CNVD 提醒相关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-2013-13305>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13174>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13176>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13227>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13206>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13207>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-13208>

5、Real Estate PHP Scrip listingid 参数 SQL 注入漏洞

Real Estate PHP Script 是一款基于 WEB 的 PHP 脚本应用。本周，该产品被披露存在一个综合评级为“高危”的 SQL 注入漏洞。Real Estate PHP Script 未能正确过滤用户提交的 listingid 参数，远程攻击者利用漏洞提交特制的 SQL 查询，可获取或操作数据库信息。目前，互联网上已经出现了针对该漏洞的攻击代码，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-2013-13265>

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-2013-13322	Splunk 告警测试脚本任意命令执行漏洞	高	用户可联系厂商获得相应的升级或补丁程序： http://www.splunk.com
CNVD-2013-13324	elproLOG MONITOR WebAccess sql 注入漏洞	高	暂无
CNVD-2013-13303	X2CRM 'file'本地文件包含漏洞	高	用户可联系厂商获得相应的升级或补丁程序： http://www.x2engine.com/ http://x2community.com/index.php?topic/1005-x2crm-35-released/
CNVD-2013-13306	AspxCommerce'LogoHandler.ashx' 模块任意文件上传漏洞	高	暂无
CNVD-2013-13317	Share KM 远程拒绝服务漏洞	高	暂无
CNVD-2013-13318	Apache Struts 远程代码执行漏洞	高	用户可联系厂商获得相应的升级或补丁程序： http://struts.apache.org/release/2.3.x/docs/s2-019.html http://struts.apache.org/download.cgi#struts23152
CNVD-2013-13262	SolarWinds Server and Application Monitor ActiveX 缓冲区溢出漏洞	高	暂无

CNVD-2013-13266	NETELLER Direct Payment API 参数操作安全绕过漏洞	高	暂无
CNVD-2013-13276	FFmpeg / Libav wtvfile_open2 函数文件名长度检查整数溢出漏洞	高	用户可联系厂商获得相应的升级或补丁程序： http://git.libav.org/?p=libav.git;a=commit;h=83c285f88016b087c2f0f4b9ef356ad8ef12d947 http://git.videolan.org/?p=ffmpeg.git;a=commit;h=83c285f88016b087c2f0f4b9ef356ad8ef12d947
CNVD-2013-13290	AjaXplorer 'checkInstall.php'远程命令执行漏洞	高	用户可联系厂商获得相应的升级或补丁程序： http://ajaxplorer.info/

表 3 部分高危漏洞列表

小结：本周，Apple、IBM 和 Cisco 多款产品以及 WordPress 多款插件被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息，执行任意代码，发起拒绝服务攻击。此外，Real Estate PHP Script 应用被披露存在一个高危零日漏洞，建议相关用户应随时关注厂商主页，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、Microsoft 发布升级程序，修补 Microsoft Internet Explorer 8 产品安全漏洞

Internet Explorer 是微软公司推出的一款网页浏览器。本周，Microsoft 发布升级程序，修补 Microsoft Internet Explorer 8 产品存在的内存破坏漏洞，攻击者利用漏洞可造成释放后重用。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安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/39666>

本周要闻速递

1. Android 新漏洞发现同 WiFi 网络可窃取 SD 卡内容

根据安全研究人员发布的最新公告显示又找到一个能够威胁大部分 Android 设备的最新漏洞。该漏洞主要出现在 WebView 编程接口方面，开发者能够通过该接口来让本地应用实现网页端的相关功能。如果本地应用在访问网络进行数据传输的时候，将能够被在相同 WiFi 网络环境下的黑客轻松攻击。安全研究公司 MWR InfoSecurity 表示“目前发现的该漏洞至少能够实现远程下载手机 SD 卡上的内容，并能够捕获应用程序的相

关数据等功能。”此外研究者还对目前 Google Play 商城出售的最畅销 100 款应用进行了检测，发现有 62 款应用存在“潜在”威胁，非常容易受到该漏洞的攻击。最后安全专家表示鉴于目前 Android 系统都是由各个 OEM 厂商自行推送更新，导致固件升级延误，谷歌应该从应用程序方面着手，要求新应用应该对 WebView 数据进行 SSL 加密。

参考链接：<http://digi.163.com/13/0928/07/99RHAPM600162OUT.html>

2. 苹果发布 iOS 7.0.2 更新修复锁屏密码安全漏洞

据报道，在 iOS 7 发布几小内后，就有用户发现了该漏洞，该漏洞会使任何人直接访问用户应用及相关数据。苹果公司上周曾表示，它正在修复这一漏洞，但没有提供修复完毕、发布更新的具体时间。随着安全修复更新程序的推出，苹果称其在密码输入时重新引入了希腊键盘选项，而此前苹果发布的 iOS 7 显然没有这项功能。移动设备提供的密码锁屏方式似乎有些落伍和多余。本月初，苹果在发布 iPhone 5s 时曾表示，仅有大约一半的智能手机用户真正启用了密码安全功能。而苹果在最新的 iOS 设备上推出了指纹扫描技术，确保用户不必输入密码而用指纹替代。预计苹果将把这一安全功能用于其未来所有设备。

参考链接：http://tech.ifeng.com/telecom/detail_2013_09/27/29930863_0.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

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 国际合作伙伴”关系。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999