国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 09 月 21 日-2015 年 09 月 27 日 **2015 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 184 个，其中高危漏洞 51 个、中危漏洞 118 个、低危漏洞 15 个。上述漏洞中，可利用来实施远程攻击的漏洞有 161 个。本周收录的漏洞中，已有 170 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。其中互联网上出现“UPnP Filet-O-Firewall 协议存在漏洞”、“Phillipine Long Distance Telephone SpeedSurf 504 AN 和 Kasda KW58293 拒绝服务漏洞”等零日漏洞，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 184 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、天融信、安天实验室、启明星辰等单位报送数量较多。此外，乌云、漏洞盒子、High-Tech Bridge Security Research 及白帽子向 CNVD 提交了 681 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎(补天平台)	339	339
天融信	180	0
安天实验室	161	0
启明星辰	136	0
绿盟科技	44	0

恒安嘉新	12	0
乌云	306	306
漏洞盒子	33	33
High-Tech Bridge Security Research	1	1
个人	2	2
报送总计	1214	681
录入总计	184（去重）	681

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、PHP、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	91	49%
2	PHP	10	5%
3	Cisco	9	5%
4	Google	7	4%
5	Symantec	6	3%
6	WordPress	5	3%
7	Drupal	5	3%
8	NTP	4	2%
9	Securifi	4	2%
10	其他	43	24%

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 184 个漏洞。其中操作系统漏洞 94 个，应用程序漏洞 56 个，网络设备漏洞 18 个，Web 应用漏洞 14 个，安全产品漏洞 1 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	94
应用程序漏洞	56
网络设备漏洞	18

Web 应用漏洞	14
安全产品漏洞	1
数据库漏洞	1

表 3 漏洞按影响类型统计表

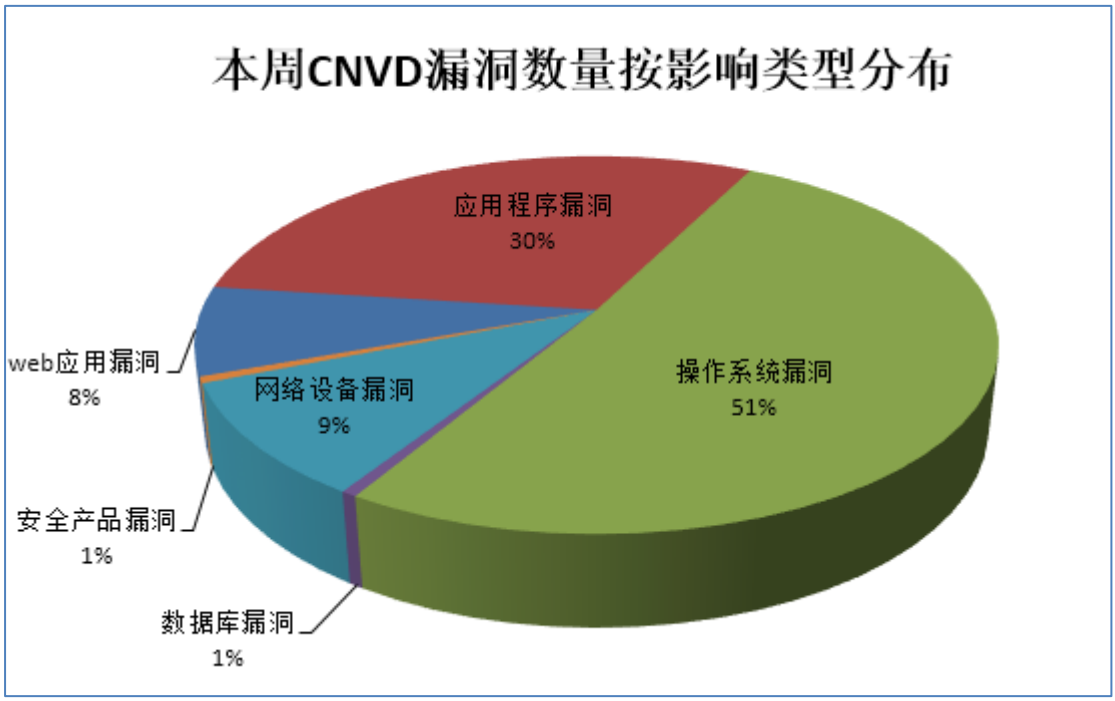

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 19 个电信行业漏洞、93 个移动互联网行业漏洞、1 个工系统行业漏洞（如下图表所示）。其中，“Huawei UAP2105 命令注入漏洞、PostgreSQL 存在多个漏洞、Apple iOS IOAcceleratorFamily 内存破坏漏洞、Apple iOS IOHIDFamily 内存破坏漏洞、Apple iOS 内核内存破坏漏洞、Apple iOS 内核内存破坏漏洞（CNVD-2015-06075、CNVD-2015-06076、CNVD-2015-06194、CNVD-2015-06193）、Apple iOS IOMobileFrameBuffer 内存破坏漏洞、Apple iOS dyld 内存破坏漏洞、Apple iOS DiskImages 内存破坏漏洞、Apple iOS SQLite 存在多个未明漏洞、Apple iOS 进程修改漏洞、Apple iOS libpthread 内核内存破坏漏洞、Apple iOS 内核内存破坏漏洞（CNVD-2015-06195）、Google Android 整数溢出漏洞（CNVD-2015-06209、CNVD-2015-06215）、Google Android Stagefright 整数溢出漏洞、Google Android 整数溢出漏洞（CNVD-2015-06217）、Google Android libcutils 'native_handle_ create()'函数整数溢出漏洞、S-Smart Software Solutions CODESYS Gateway Server 堆缓冲区溢出漏洞、Huawei UAP2105 命令注入漏洞”的综合评级为“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	是否有

			等级	补丁
电信	CNVD-2015-06071	UPnP Filet-O-Firewall 协议存在漏洞	高	否
电信	CNVD-2015-06094	Securifi Almond 访问限制绕过漏洞	中	是
电信	CNVD-2015-06095	Securifi Almond 跨站请求伪造漏洞（CNVD-2015-06095）	中	是
电信	CNVD-2015-06093	Securifi Almond 跨站请求伪造漏洞	中	是
电信	CNVD-2015-06092	Securifi Almond 安全绕过漏洞	中	是
电信	CNVD-2015-06098	Phillipine Long Distance Telephone SpeedSurf 504AN 和 Kasda KW58293 拒绝服务漏洞	高	否
电信	CNVD-2015-06099	Phillipine Long Distance Telephone SpeedSurf 504AN 和 Kasda KW58293 跨站脚本漏洞	中	否
电信	CNVD-2015-06101	Phillipine Long Distance Telephone SpeedSurf 504AN 和 Kasda KW58293 跨站请求伪造漏洞	中	否
电信	CNVD-2015-06110	Huawei UAP2105 命令注入漏洞	高	是
电信	CNVD-2015-06114	MediabridgeMedialink Wireless-N Broadband Router MWN-WAPR300N 跨站请求伪造漏洞	中	否
电信	CNVD-2015-06115	MediabridgeMedialink Wireless-N Broadband Router MWN-WAPR300N 安全绕过漏洞	中	否
电信	CNVD-2015-06116	MediabridgeMedialink Wireless-N Broadband Router MWN-WAPR300N 安全绕过漏洞（CNVD-2015-06116）	中	否
电信	CNVD-2015-06132	Belkin N600 DB Wireless Dual Band N+跨站请求伪造漏洞	中	否
电信	CNVD-2015-06131	Belkin N600 DB Wireless Dual Band N+安全绕过漏洞	中	否
电信	CNVD-2015-06130	Belkin N600 DB Wireless Dual Band N+管理界面无密码设置漏洞	中	否
电信	CNVD-2015-06203	PostgreSQL 存在多个漏洞	高	是
电信	CNVD-2015-06206	Cisco IOS DHCPv6 服务器拒绝服务漏洞	中	是
电信	CNVD-2015-06223	Cisco Nexus 9000 NX-OS 远程拒绝服务漏洞	低	否
电信	CNVD-2015-06220	3S-Smart Software Solutions CODESYS Gateway Server 堆缓冲区溢出漏洞	高	是
移动互联网	CNVD-2015-06080	Apple iOS Apple Pay terminal 敏感交易信息获取漏洞	中	是
移动互联网	CNVD-2015-06081	Apple iOS iOS 备份密码重置漏洞	低	是
移动互联网	CNVD-2015-06082	Apple iOS NSURL 证书校验漏洞	中	是

移动互联网	CNVD-2015-06083	Apple iOS 敏感用户信息泄露漏洞	中	是
移动互联网	CNVD-2015-06072	Apple iOS IOAcceleratorFamily 内存破坏漏洞	高	是
移动互联网	CNVD-2015-06073	Apple iOS IOHIDFamily 内存破坏漏洞	高	是
移动互联网	CNVD-2015-06074	Apple iOS 内核内存破坏漏洞	高	是
移动互联网	CNVD-2015-06075	Apple iOS 内核内存破坏漏洞（CNVD-2015-06075）	高	是
移动互联网	CNVD-2015-06076	Apple iOS 内核内存破坏漏洞（CNVD-2015-06076）	高	是
移动互联网	CNVD-2015-06077	Apple iOS IOMobileFrameBuffer 内存破坏漏洞	高	是
移动互联网	CNVD-2015-06078	Apple iOS IOStorageFamily 内存信息泄露漏洞	低	是
移动互联网	CNVD-2015-06079	Apple iOS keychain 信息泄露漏洞	低	是
移动互联网	CNVD-2015-06084	Apple iOS 特殊文本文件代码执行漏洞	中	是
移动互联网	CNVD-2015-06085	Apple iOS dyld 内存破坏漏洞	高	是
移动互联网	CNVD-2015-06086	Apple iOS DiskImages 内存破坏漏洞	高	是
移动互联网	CNVD-2015-06087	Apple iOS 可执行程序代码签名校验漏洞	中	是
移动互联网	CNVD-2015-06088	Apple iOS Game Center 信息泄露漏洞	中	是
移动互联网	CNVD-2015-06089	Apple iOS ITMS 链接拒绝服务漏洞	中	是
移动互联网	CNVD-2015-06090	Apple iOS 敏感内存信息泄露漏洞（CNVD-2015-06090）	中	是
移动互联网	CNVD-2015-06106	Nokia Solutions And Networks 跨站脚本漏洞	中	否
移动互联网	CNVD-2015-06121	Apple iOS WebKit 内存破坏漏洞	中	是
移动互联网	CNVD-2015-06122	Apple iOS 音频文件处理拒绝服务漏洞	中	是
移动互联网	CNVD-2015-06123	Apple iOS WebKit 内存破坏漏洞（CNVD-2015-06123）	中	是
移动互联网	CNVD-2015-06124	Apple iOS WebKit 内存破坏漏洞（CNVD-2015-06124）	中	是
移动互联网	CNVD-2015-06125	Apple iOS WebKit 内存破坏漏洞（CNVD-2015-06125）	中	是
移动互联网	CNVD-2015-06126	Apple iOS WebKit 内存破坏漏洞（CNVD-2015-06126）	中	是
移动互联网	CNVD-2015-06127	Apple iOS WebKit 内存破坏漏洞（CNVD-2015-06127）	中	是
移动互联网	CNVD-2015-06135	Apple iOS Webkit 信息泄露漏洞	中	是
移动互联网	CNVD-2015-06136	Apple iOS Webkit 'canvas'元素图像处理信息泄露漏洞	中	是
移动互联网	CNVD-2015-06145	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06145）	中	是
移动互联网	CNVD-2015-06146	Apple iOS Webkit 内存破坏漏洞（CNV	中	是

		D-2015-06146）		
移动互联网	CNVD-2015-06147	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06147）	中	是
移动互联网	CNVD-2015-06141	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06141）	中	是
移动互联网	CNVD-2015-06140	Apple iOS Webkit URL 处理漏洞	中	是
移动互联网	CNVD-2015-06139	Apple iOS Webkit 密码输入上下文漏洞	中	是
移动互联网	CNVD-2015-06144	Apple iOS Webkit 重定向恶意域漏洞	低	是
移动互联网	CNVD-2015-06143	Apple iOS Webkit 恶意跨域样式表达处理漏洞	中	是
移动互联网	CNVD-2015-06142	Apple iOS Webkit Performance API 行为跟踪漏洞	中	是
移动互联网	CNVD-2015-06148	Apple iOS 恶意代码恶意 COOKIE 设置漏洞	中	是
移动互联网	CNVD-2015-06152	Apple iOS Safari 任意 URL 显示漏洞	中	是
移动互联网	CNVD-2015-06153	Apple iOS Safari 任意 URL 显示漏洞（CNVD-2015-06153）	中	是
移动互联网	CNVD-2015-06154	Apple iOS Safari 任意 URL 显示漏洞（CNVD-2015-06154）	中	是
移动互联网	CNVD-2015-06155	Apple iOS SQLite 存在多个未明漏洞	高	是
移动互联网	CNVD-2015-06159	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06159）	中	是
移动互联网	CNVD-2015-06160	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06160）	中	是
移动互联网	CNVD-2015-06161	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06161）	中	是
移动互联网	CNVD-2015-06169	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06169）	中	是
移动互联网	CNVD-2015-06166	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06166）	中	是
移动互联网	CNVD-2015-06167	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06167）	中	是
移动互联网	CNVD-2015-06168	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06168）	中	是
移动互联网	CNVD-2015-06162	Apple iOS HSTS 绕过敏感数据泄露漏洞	中	是
移动互联网	CNVD-2015-06163	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06163）	中	是
移动互联网	CNVD-2015-06164	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06164）	中	是
移动互联网	CNVD-2015-06165	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06165）	中	是
移动互联网	CNVD-2015-06175	Apple iOS cookie 处理不当漏洞	中	是

移动互联网	CNVD-2015-06172	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06172）	中	是
移动互联网	CNVD-2015-06173	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06173）	中	是
移动互联网	CNVD-2015-06174	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06174）	中	是
移动互联网	CNVD-2015-06176	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06176）	中	是
移动互联网	CNVD-2015-06177	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06177）	中	是
移动互联网	CNVD-2015-06171	Apple iOS 敏感信息泄露漏洞（CNVD-2015-06171）	中	是
移动互联网	CNVD-2015-06170	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06170）	中	是
移动互联网	CNVD-2015-06185	Apple iOS 未保护 multipeer 数据泄露漏洞	中	是
移动互联网	CNVD-2015-06183	Apple iOS 内存未初始化漏洞	中	是
移动互联网	CNVD-2015-06184	Apple iOS App 应用通信截取漏洞	中	是
移动互联网	CNVD-2015-06181	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06181）	中	是
移动互联网	CNVD-2015-06182	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06182）	中	是
移动互联网	CNVD-2015-06180	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06180）	中	是
移动互联网	CNVD-2015-06179	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06179）	中	是
移动互联网	CNVD-2015-06178	Apple iOS Webkit 内存破坏漏洞（CNVD-2015-06178）	中	是
移动互联网	CNVD-2015-06194	Apple iOS 内核内存破坏漏洞（CNVD-2015-06194）	高	是
移动互联网	CNVD-2015-06193	Apple iOS 内核内存破坏漏洞（CNVD-2015-06193）	高	是
移动互联网	CNVD-2015-06192	Apple iOS 进程修改漏洞	高	是
移动互联网	CNVD-2015-06191	Apple iOS App 缓存数据泄露漏洞	低	是
移动互联网	CNVD-2015-06190	Apple iOS xnu TCP 报文头校验漏洞	中	是
移动互联网	CNVD-2015-06189	Apple iOS IPv6 路由通告处理不充分漏洞	低	是
移动互联网	CNVD-2015-06187	Apple iOS XNU 内存泄露漏洞	低	是
移动互联网	CNVD-2015-06188	Apple iOS libpthread 内核内存破坏漏洞	高	是
移动互联网	CNVD-2015-06186	Apple iOS mail 发送者地址处理漏洞	中	是
移动互联网	CNVD-2015-06195	Apple iOS 内核内存破坏漏洞（CNVD-2015-06195）	高	是
移动互联网	CNVD-2015-06196	Apple iOS checkint division 溢出漏洞	中	是

移动互联网	CNVD-2015-06197	Apple iOS 跨域 COOKIE 处理漏洞	中	是
移动互联网	CNVD-2015-06198	Apple iOS Safari 用户接口伪造漏洞	中	是
移动互联网	CNVD-2015-06202	Apple iOS 扩展校验漏洞	中	是
移动互联网	CNVD-2015-06199	Apple iOS Safari 用户接口伪造漏洞（CNVD-2015-06199）	中	是
移动互联网	CNVD-2015-06201	Apple iOS 锁屏绕过音频消息应答漏洞	低	是
移动互联网	CNVD-2015-06200	Apple iOS 私有 API 调用漏洞	中	是
移动互联网	CNVD-2015-06209	Google Android 整数溢出漏洞（CNVD-2015-06209）	高	是
移动互联网	CNVD-2015-06214	Google Android 拒绝服务漏洞	中	是
移动互联网	CNVD-2015-06215	Google Android 整数溢出漏洞（CNVD-2015-06215）	高	是
移动互联网	CNVD-2015-06216	Google Android Stagefright 整数溢出漏洞	高	是
移动互联网	CNVD-2015-06217	Google Android 整数溢出漏洞（CNVD-2015-06217）	高	是
移动互联网	CNVD-2015-06218	Google Android libcutils 'native_handle_create()'函数整数溢出漏洞	高	是
工控系统	CNVD-2015-06219	Advantech WebAccess 堆缓冲区溢出漏洞	中	是

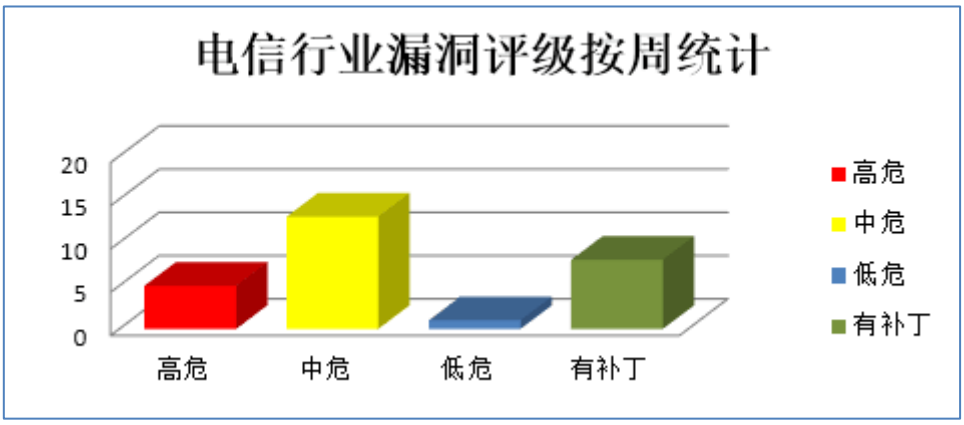

图 1 电信行业漏洞统计

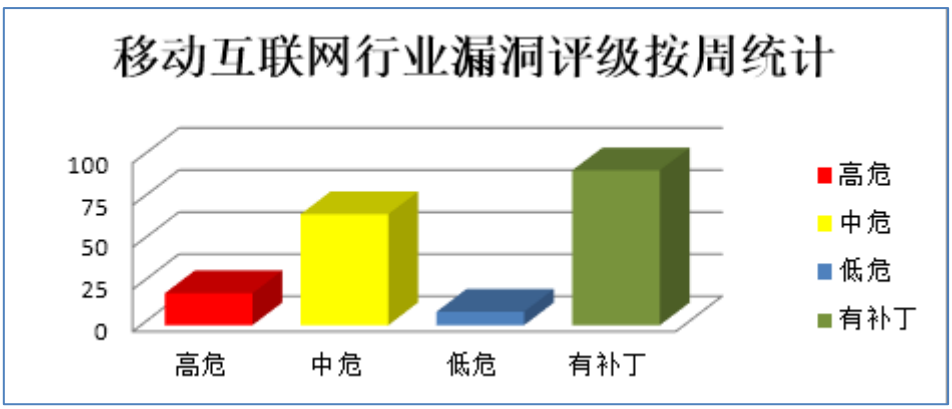

图 2 移动互联网行业漏洞统计

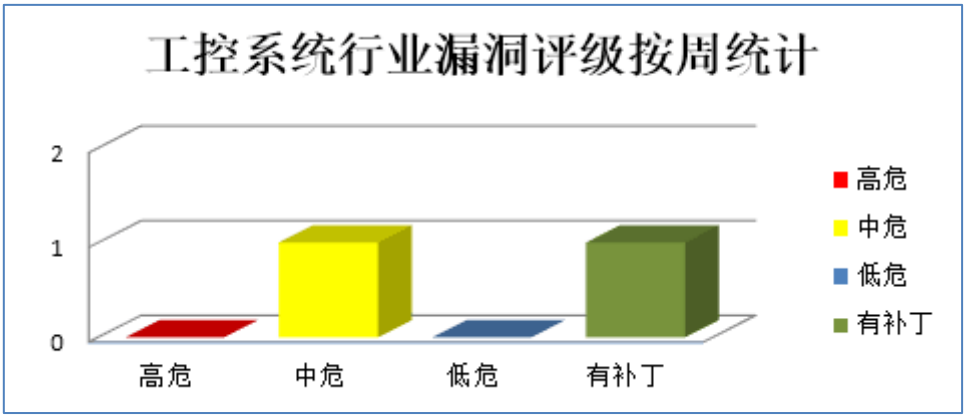

图 3 工控系统行业漏洞统计

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、 Apple 产品安全漏洞

Apple iOS 是一款运行在苹果 iPhone 和 iPod touch 设备上的操作系统。本周，部分产品被披露存在内存破坏漏洞。攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Apple iOS 内核内存破坏漏洞（CNVD-2015-06193、CNVD-2015-06194、CNVD-2015-06195、CNVD-2015-06076、CNVD-2015-06075、CNVD-2015-06074）、Apple iOS IOHIDFamily 内存破坏漏洞、Apple iOS IOAcceleratorFamily 内存破坏漏洞。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-2015-06193

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06194

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06195

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06076

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06075

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06074

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06073

http://www.cnvd.org.cn/flaw/show/CNVD-2015-06072

2、 Google 产品安全漏洞

Android 是基于 Linux 开放性内核的操作系统，是 Google 公司在 2007 年 11 月 5 日公布的手机操作系统。本周，该产品被披露存在拒绝服务、安全限制绕过和整数溢出漏洞。攻击者利用漏洞可发起拒绝服务攻击、绕过某些安全限制并执行未授权操作。

CNVD 收录的相关漏洞包括：Google Android libcutils 'native_handle_ create()'函数

整数溢出漏洞、Google Android Stagefright 整数溢出漏洞、Google Android 安全限制绕过漏洞、Google Android 拒绝服务漏洞、Google Android 整数溢出漏洞（CNVD-2015-06209、CNVD-2015-06215、CNVD-2015-06217）。其中，除“Google Android 安全限制绕过漏洞、Google Android 拒绝服务漏洞”外，其余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-2015-06218
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06216
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06213
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06214
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06209
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06215
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06217

3、 Symantec 产品安全漏洞

Symantec Web Gateway 是一套网络内容过滤软件，该软件提供了网络内容过滤和数据泄露防护功能。本周，该产品被披露存在多个漏洞。攻击者利用漏洞可获得敏感信息、进行跨站脚本攻击、上传任意文件和执行任意命令。

CNVD 收录的相关漏洞包括：Symantec Web Gateway 代码注入漏洞（CNVD-2015-06069）、Symantec Web Gateway OS 命令注入漏洞（CNVD-2015-06070）、Symantec Web Gateway SQL 注入漏洞（CNVD-2015-06066）、Symantec Web Gateway 跨站脚本漏洞（CNVD-2015-06067）、Symantec Web Gateway 任意文件上传漏洞、Symantec Web Gateway 安全绕过漏洞。其中，除“Symantec Web Gateway SQL 注入漏洞（CNVD-2015-06066）、Symantec Web Gateway 跨站脚本漏洞（CNVD-2015-06067）”外，其余漏洞的综合评级为“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-2015-06069
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06070
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06066
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06067
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06068
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06065

4、 Cisco 产品安全漏洞

Cisco Unity Connection 是一个语音留言平台；Cisco Secure Access Control System 是访问策略控制平台；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 Prime Collaboration Provisioning 是一套基于 Web 的下一代通信服务解

决方案；Cisco Prime Collaboration Assurance 是美国思科（Cisco）公司的一套企业协作网络管理解决方案；Cisco TelePresence Server Software 是一套视频会议解决方案。本周，上述产品被披露存在信息泄露、SQL 注入、拒绝服务和缓冲区溢出漏洞。攻击者利用漏洞可获得敏感信息、发起拒绝服务攻击和执行任意代码。

CNVD 收录的相关漏洞包括：Cisco Prime Collaboration Provisioning 访问控制绕过漏洞、Cisco Prime Collaboration Assurance 存在漏洞、Cisco Prime Collaboration Assurance 信息泄露漏洞、Cisco TelePresence Server Software API 缓冲区溢出漏洞、Cisco IOS DHCPv6 服务器拒绝服务漏洞、Cisco Prime Collaboration Assurance 信息泄露漏洞（CNVD-2015-06129）、Cisco Unity Connection Web Interface SQL 注入漏洞、Cisco Secure Access Control Server SSH 登录拒绝服务漏洞。其中，“Cisco Prime Collaboration Provisioning 访问控制绕过漏洞、Cisco Prime Collaboration Assurance 存在漏洞、Cisco Prime Collaboration Assurance 信息泄露漏洞、Cisco TelePresence Server Software API 缓冲区溢出漏洞”的综合评级均为“高危”。目前，除“Cisco Unity Connection Web Interface SQL 注入漏洞、Cisco Secure Access Control Server SSH 登录拒绝服务漏洞”外，厂商已发布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-2015-06221
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06222
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06113
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06133
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06206
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06129
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06208
http://www.cnvd.org.cn/flaw/show/CNVD-2015-06207

5、 UPnP Filet-O-Firewall 协议存在漏洞

UPnP 是通用即插即用论坛推广的一套网络协议。该协议可实现家庭网络和公司网络中的各种设备相互连接，并简化相关网络的实现。本周，UPnP 被披露存在高危漏洞。攻击者利用该漏洞可更改路由器配置。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-2015-06071

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-2015-06205	Avira Management Console 内存错误引用漏洞	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.avira.com/en/for-business-avira-management-console
CNVD-2015-06157	WordPress WP Symposium 插件 'forum_functions.php' SQL 注入漏洞	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.wpsymposium.com/
CNVD-2015-06225	PHP 'spl_array.c’远程代码执行漏洞	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://php.net/ChangeLog-5.php
CNVD-2015-06226	PHP 远程代码执行漏洞（CNVD-2015-06226）	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://php.net/ChangeLog-5.php
CNVD-2015-06228	Hancom Hangul Word Processor 远程代码执行漏洞	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://www.hancom.com/
CNVD-2015-06220	3S-Smart Software Solutions CODESYS Gateway Server 堆缓冲区溢出漏洞	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： https://www.codesys.com/download/download-center.html
CNVD-2015-06212	IBM QRadar Security Information and Event Manager Unspecified 命令注入漏洞	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-01.ibm.com/support/docview.wss?uid=swg21965813
CNVD-2015-06238	Kaspersky Anti-Virus 栈缓冲区溢出漏洞	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.kaspersky.com/
CNVD-2015-06211	TeikoFarol Web 应用程序 SQL 注入漏洞	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.teiko.com.br/pt/solucoes/infraestrutura-em-ti/farol
CNVD-2015-06117	NTP 存在多个任意文件覆盖漏洞	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： https://bodhi.fedoraproject.org/updates/FEDORA-2015-14211 https://bodhi.fedoraproject.org/updates/FEDORA-2015-14212

			https://bodhi.fedoraproject.org/updates/FEDORA-2015-14213

表 3 部分高危漏洞列表

小结：本周，移动互联网行业漏洞较多，主要原因是收录了 Apple IOS 产品存在的多个漏洞。其中，Apple 部分产品被披露存在内存破坏漏洞，攻击者利用漏洞可执行任意代码。此外，Google、Symantec、Cisco 多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息、进行跨站脚本攻击、执行未授权操作、上传任意文件、发起拒绝服务攻击和执行任意命令。另外，UPnP 被披露存在一个高危零日漏洞，攻击者利用该漏洞可更改路由器设置。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 UrbanCode Build/SIEM 产品漏洞

IBM UrbanCode Build 是一款持续集成和构建管理服务器；IBM QRadar Security Information and Event Manager（SIEM）是一套数据整合的解决方案。

本周，IBM 修补了上述产品存在的跨站脚本和命令注入漏洞，避免攻击者利用漏洞进行跨站脚本攻击和执行任意命令。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/64482

http://www.cnvd.org.cn/patchInfo/show/64463

本周要闻速递

1. 苹果手表 watchOS 2 更新

苹果手表 watchOS 2 更新，解决了多个安全问题。新系统修复的漏洞包括：存在于多个组件中的远程代码执行漏洞，以及一些 CFNetwork 证书验证的问题；操作系统的动态链接器漏洞；开发人员使用核心服务框架作为网络协议抽象库的漏洞；watchOS 处理代理连接漏洞；需要物理访问到 iOS 设备的加密问题。苹果还修补了不少 watchOS 内核的问题，其中多涉及破坏内存的漏洞，这些漏洞会让攻击者获得内核权限然后执行代码，其中就有允许本地攻击者控制堆栈 cookies。苹果还修补了内核内存泄露的漏洞以及一个拒绝服务问题。

参考链接：http://www.freebuf.com/news/79397.html

2. 利用浏览器 Cookie 绕过 HTTPS 并窃取私人信息

近期，一个存在于主要浏览器的 Web cookie 中的严重漏洞被发现，它使安全的浏

览方式（HTTPS）容易遭受中间人攻击。此外，大部分 Web 网站和流行的开源应用程序中可能都含有 Cookie 注入漏洞。包括：谷歌、亚马逊、eBay、苹果、美国银行、Bit Bucket、中国建设银行、中国银联、京东、phpMyAdmin 以及 MediaWiki。此外，受影响的主流 Web 浏览器包括以下浏览器的早期版本：苹果的 Safari、Mozilla 的 Firefox、谷歌的 Chrome、微软的 IE 浏览器、微软的 Edge、Opera。目前，供应商现在已经解决了这个问题。

参考链接：http://www.freebuf.com/news/79934.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