国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 02 月 02 日-2015 年 02 月 08 日 **2015 年第 6 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 168 个，其中高危漏洞 59 个、中危漏洞 97 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 153 个。本周收录的漏洞中，已有 140 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“Zero CMS 存在多个 SQL 注入漏洞”、“NPDS Revolution 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 7 家成员单位及个人报送了本周收录的全部 168 个漏洞。报送情况如表 1 所示。其中，奇虎 360、天融信、启明星辰、恒安嘉新、绿盟科技等单位报送数量较多。此外，CNCERT 各分中心、上海天泰网络技术有限公司及白帽子向 CNVD 提交了 1214 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	1205	1205
天融信	130	0
启明星辰	111	0
恒安嘉新	97	0
绿盟科技	94	0
安天实验室	49	0

东软	3	0
上海天泰网络技术有限公司	1	1
CNCERT 福建分中心	4	4
CNCERT 宁夏分中心	1	1
个人	3	3
报送总计	1698	1214
录入总计	168（去重）	1214

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、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	39	23%
2	Cisco	13	8%
3	WordPress	7	4%
4	IBM	7	4%
5	Fortinet	7	4%
6	Google	6	4%
7	Linux	4	2%
8	Microsoft	2	1%
9	Adobe	2	1%
10	其他	81	49%

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 168 个漏洞。其中应用程序漏洞 79 个，WEB 应用漏洞 20 个，操作系统漏洞 48 个，网络设备漏洞 20 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	79
WEB 应用漏洞	20
操作系统漏洞	48

数据库漏洞	0
网络设备漏洞	20
安全产品漏洞	1

表 3 漏洞按影响类型统计表

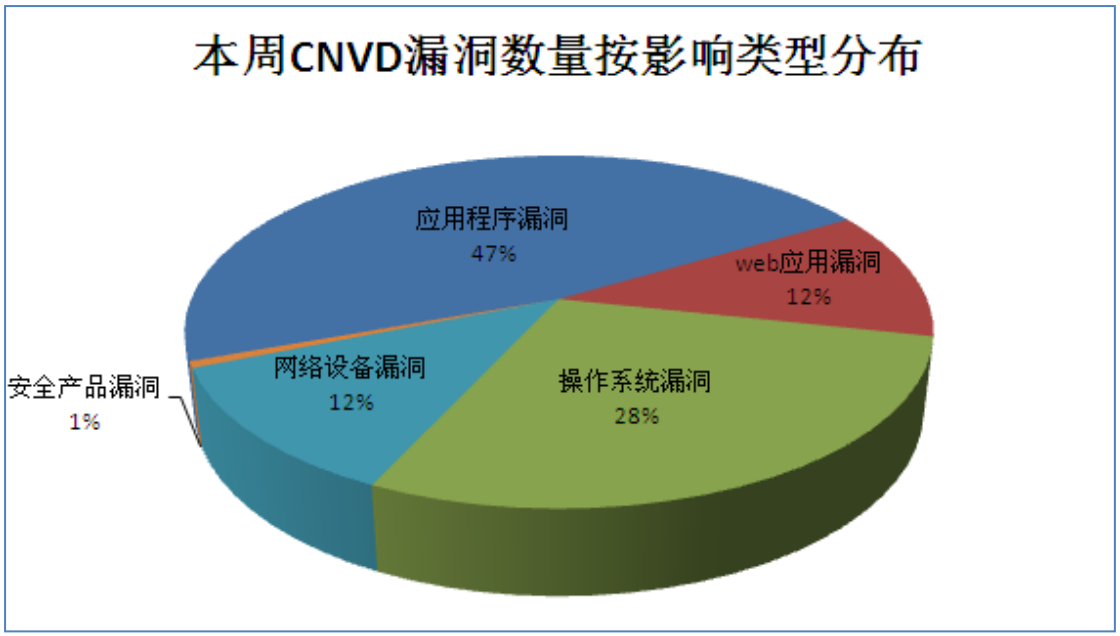

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 15 个电信行业漏洞，17 个移动互联网行业漏洞，2 个工控系统行业漏洞（如下图表所示）。其中，“Huawei Quidway Switch 权限提升漏洞、Apple TV 和 iOS .dfont 文件内存破坏漏洞、Apple TV 和 iOS XML 解析器缓冲区溢出漏洞、Apple TV 和 iOS IOAcceleratorFamily 资源列表处理拒绝服务漏洞、Apple TV 和 iOS IOHIDFamily 缓冲区溢出漏洞、Apple TV 和 iOS 应用程序安装处理安全绕过漏洞、Apple TV 和 iOS IOHIDFamily 资源队列元数据校验漏洞、Apple TV 和 iOS IOHIDFamily 事件队列空指针引用漏洞、Apple TV 和 iOS 进程间通信类型混淆漏洞、Apple TV 和 iOS 内核共享内存子系统权限提升漏洞、Apple TV 和 iOS AFC 符号链接漏洞”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-2015-00807	HP LaserJet Printers 存在多个权限绕过漏洞	中	否
电信	CNVD-2015-00835	D-Link DSL-2740R Web 界面身份验证绕过漏洞	中	否
电信	CNVD-2015-00842	Cisco WebEx Meetings Server 跨站请求伪造漏洞（CNVD-2015-00842）	中	否

电信	CNVD-2015-00841	Cisco WebEx Meetings Server 信息泄露漏洞（CNVD-2015-00841）	中	是
电信	CNVD-2015-00844	Siemens SCALANCE X-200IRT Web 服务器会话劫持漏洞	中	是
电信	CNVD-2015-00873	IBM WebSphere Message Broker 和 IBM Integration Bus 信息泄露漏洞	中	是
电信	CNVD-2015-00883	Asus RT-N10 Plus Router 'flag'参数跨站脚本漏洞	中	否
电信	CNVD-2015-00881	多个 ASUS RT 路由器跨站请求伪造漏洞	中	是
电信	CNVD-2015-00880	ASUS RT Series Routers 存在未明命令注入漏洞	中	是
电信	CNVD-2015-00878	I-O DATA DEVICE NP-BBRM 拒绝服务漏洞	中	否
电信	CNVD-2015-00894	Cisco WebEx Meetings Server 用户枚举漏洞（CNVD-2015-00894）	中	是
电信	CNVD-2015-00909	Huawei Quidway Switch 权限提升漏洞	高	是
电信	CNVD-2015-00918	多个 Cisco 产品跨站脚本漏洞	中	是
电信	CNVD-2015-00933	Huawei Quidway Switches 远程安全绕过漏洞	中	是
电信	CNVD-2015-00934	Cisco NX-OS 软件本地拒绝服务漏洞	中	是
移动互联网	CNVD-2015-00848	Apple TV 和 iOS 企业签名应用安全绕过漏洞	中	是
移动互联网	CNVD-2015-00849	Apple iOS 滚动栏边界处理 UI 伪造漏洞	中	是
移动互联网	CNVD-2015-00857	Apple TV 和 iOS 字体文件处理缓冲区溢出漏洞	中	是
移动互联网	CNVD-2015-00856	Apple TV 和 iOS .dfont 文件内存破坏漏洞	高	是
移动互联网	CNVD-2015-00855	Apple TV 和 iOS XML 解析器缓冲区溢出漏洞	高	是
移动互联网	CNVD-2015-00854	Apple TV 和 iOS IOAcceleratorFamily 资源列表处理拒绝服务漏洞	高	是
移动互联网	CNVD-2015-00853	Apple TV 和 iOS IOHIDFamily 缓冲区溢出漏洞	高	是
移动互联网	CNVD-2015-00861	Apple TV 和 iOS 应用程序安装处理安全绕过漏洞	高	是
移动互联网	CNVD-2015-00866	Apple TV 和 iOS PDF 处理整数溢出漏洞	中	是
移动互联网	CNVD-2015-00860	Apple TV 和 iOS IOHIDFamily 资源队列元数据校验漏洞	高	是
移动互联网	CNVD-2015-00862	Apple TV 和 iOS IOHIDFamily 事件队列空指针引用漏洞	高	是
移动互联网	CNVD-2015-00863	Apple TV 和 iOS API 相关内核扩展信息泄露漏洞	中	是

移动互联网	CNVD-2015-00864	Apple TV 和 iOS 进程间通信类型混淆漏洞	高	是
移动互联网	CNVD-2015-00865	Apple TV 和 iOS 内核共享内存子系统权限提升漏洞	高	是
移动互联网	CNVD-2015-00870	Apple iOS 恶意站点 Safari 沙盒限制绕过漏洞	中	是
移动互联网	CNVD-2015-00871	Apple TV 和 iOS AFC 符号链接漏洞	高	是
移动互联网	CNVD-2015-00869	Apple TV 和 iOS mach_port_kobject 内核接口信息泄露漏洞	中	是
工控系统	CNVD-2015-00844	Siemens SCALANCE X-200IRT Web 服务器会话劫持漏洞	中	是
工控系统	CNVD-2015-00896	ClearSCADA 'dbserver.exe'远程验证绕过漏洞	中	否

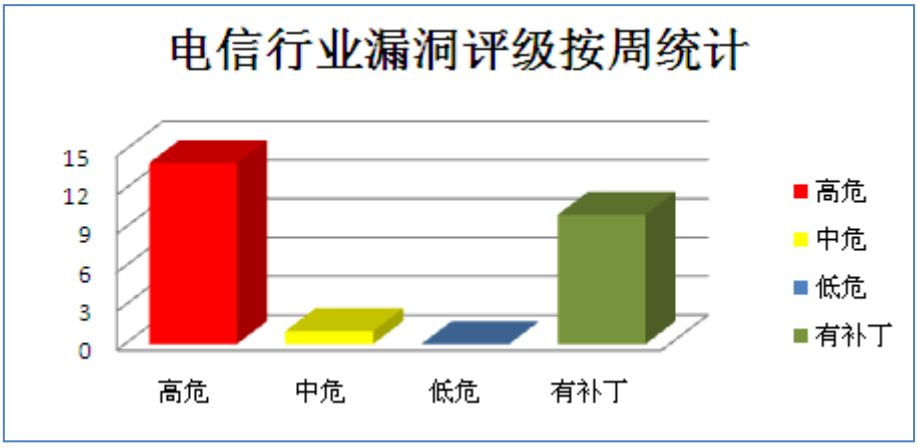

图 1 电信行业漏洞统计

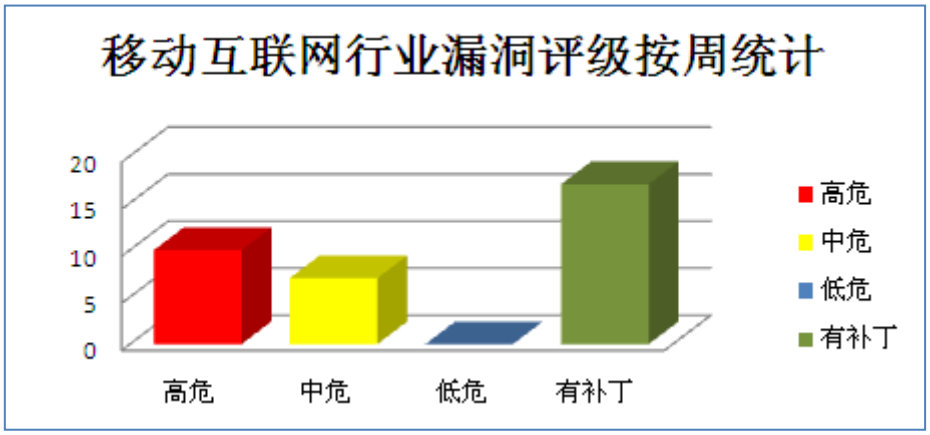

图 2 移动互联网行业漏洞统计

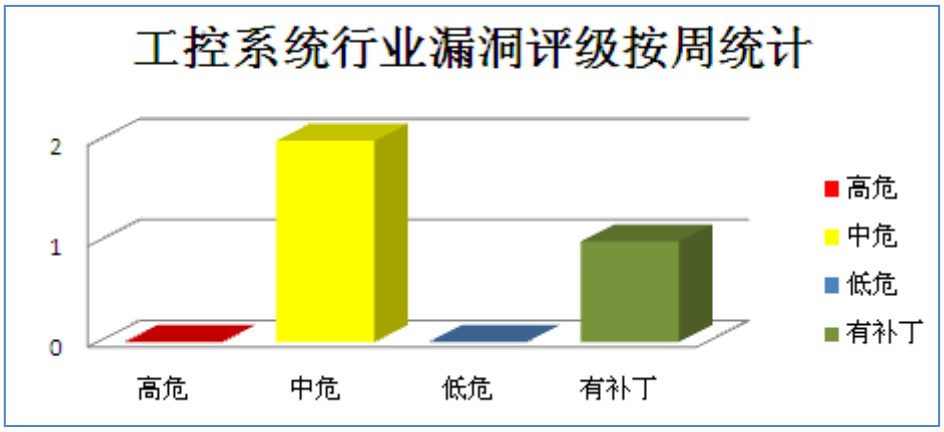

图 3 工控系统行业漏洞统计

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、 Apple 产品安全漏洞

Apple IOS 是一款运行在苹果 iPhone 和 iPod touch 设备上的最新的操作系统；Apple TV 是由苹果公司推出的一款高清电视机顶盒产品，用户可以通过 Apple TV 在线收看电视节目，也可以通过 Airplay 功能，将 iPad、iPhone、iPod 和 PC 中的照片、视频和音乐传输到电视上进行播放；Apple MAC OS X Yosemite 是苹果公司开发的最新操作系统。

CNVD 收录的相关漏洞包括： Apple TV 和 iOS .dfont 文件内存破坏漏洞、Apple TV 和 iOS XML 解析器缓冲区溢出漏洞、Apple TV 和 iOS IOAcceleratorFamily 资源列表处理拒绝服务漏洞、Apple TV 和 iOS IOHIDFamily 缓冲区溢出漏洞、Apple TV 和 iOS IOHIDFamily 资源队列元数据校验漏洞、Apple TV 和 iOS IOHIDFamily 事件队列空指针引用漏洞、Apple TV 和 iOS 内核共享内存子系统权限提升漏洞、Apple MAC OS X Yosemite 文件处理堆缓冲区溢出漏洞。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-2015-00856
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00855
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00854
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00853
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00860
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00862
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00865

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00776

2、Google 产品安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，上述产品被披露存在内存错误引用、未授权访问和拒绝服务漏洞，攻击者可利用漏洞获取敏感信息或者发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Chrome 拒绝服务漏洞（CNVD-2015-00819）、Google Chrome PDFium 内存错误引用漏洞 、Google Chrome uninstall-survey 函数未授权访问漏洞、Google Chrome PDFium 拒绝服务漏洞、Google Chrome Skia 拒绝服务漏洞（CNVD-2015-00811）、Google Chrome Blink 拒绝服务漏洞（CNVD-2015-00810）。其中，“Google Chrome Skia 拒绝服务漏洞（CNVD-2015-00811）”的漏洞综合评级为“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-2015-00819

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00820

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00821

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00812

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00811

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00810

3、IBM 产品安全漏洞

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。该产品为面向服务架构（SOA）环境和非 SOA 环境提供连通性和通用数据转换；IBM Security AppScan Standard 是美国 IBM 公司的一套 Web 应用的安全测试工具。该工具可在应用开发生命周期中进行自动化动态和静态安全漏洞扫描；IBM TRIRIGA Application Platform 是一款可用于部署 IBM TRIRIGA 应用程序的可扩充式技术平台。

CNVD 收录的相关漏洞包括： IBM WebSphere Message Broker 和 IBM Integration Bus 信息泄露漏洞、IBM Security AppScan Standard 信息泄露漏洞（CNVD-2015-00885）、IBM TRIRIGA Application Platform 安全绕过漏洞、IBM Dojo Toolkit 存在多个跨站脚本漏洞。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-2015-00873

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00885

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00831

http://www.cnvd.org.cn/flaw/show/CNVD-2015-00824

4、Cisco 产品安全漏洞

Cisco Unified IP Phone 9900 是美国思科（Cisco）公司的 9900 系列 IP 电话终端设备，该设备提供语音、视频等功能；Cisco AnyConnect Secure Mobility Client 是一个移动客户端 VPN 工具。Cisco HostScan Engine 是一个主机扫描引擎；Cisco NX-OS 是一个数据中心级的操作系统；Cisco Meraki Systems Manager 是一款云端管理解决方案；Cisco WebEx Meetings 是网络会议解决方案；Cisco Prime Service Catalog 是思科提供的通过一个单一的门户网站提供的所有服务的解决方案。

CNVD 收录的相关漏洞包括：Cisco Unified IP Phones 9900 Series 任意文件上传漏洞、多个 Cisco 产品跨站脚本漏洞、Cisco NX-OS 软件本地拒绝服务漏洞、Cisco Meraki Systems Manager HTML 注入漏洞、Cisco Meraki Systems Manager 跨站请求伪造漏洞、Cisco WebEx Meetings Server 用户枚举漏洞（CNVD-2015-00894）、Cisco WebEx Meetings Server 信息泄露漏洞（CNVD-2015-00841）、Cisco Prime Service Catalog 拒绝服务漏洞。其中“Cisco Unified IP Phones 9900 Series 任意文件上传漏洞、Cisco Prime Service Catalog 拒绝服务漏洞”的漏洞综合评级为“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-2015-00919
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00918
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00934
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00886
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00887
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00894
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00841
http://www.cnvd.org.cn/flaw/show/CNVD-2015-00825

5、Microsoft Windows User Profile 服务权限提升漏洞

Microsoft Windows 是一款由美国微软公司开发的窗口化操作系统。本周，Microsoft Windows User Profile Service 服务在验证用户权限时被披露存在综合评级为“高危”的权限提升漏洞。攻击者可以利用漏洞使 User Profile Service 服务载入与其他用户有关的注册表单元(Registry Hives)，进而提升服务权限。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-2015-00899

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-2015-00905	GNU glibc 'swscanf'远程堆缓冲区溢出漏洞	高	否

CNVD-2015-00908	Sefrengo CMS 存在多个 SQL 注入漏洞	高	否
CNVD-2015-00909	Huawei Quidway Switch 权限提升漏洞	高	目前厂商已经发布了补丁修复程序，请广大用户及时下载：http://www.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-411975.htm
CNVD-2015-00910	ClamAV 堆缓冲区溢出漏洞（CNVD-2015-00910）	高	目前厂商已经发布了补丁修复程序，请广大用户及时下载：http://blog.clamav.net/2015/01/clamav-0986-has-been-released.html
CNVD-2015-00929	McAfee Data Loss Prevention Endpoint 本地权限提升漏洞	高	目前厂商已经发布了补丁修复程序，请广大用户及时下载：http://www.mcafee.com
CNVD-2015-00932	Piwigo 存在未明 SQL 注入漏洞	高	目前厂商已经发布了补丁修复程序，请广大用户及时下载：http://piwigo.org/
CNVD-2015-00925	Libmspack 内存破坏漏洞	高	目前厂商已经发布了补丁修复程序，请广大用户及时下载：http://www.cabextract.org.uk/libmspack/#download
CNVD-2015-00927	MIT krb5 kadmind 远程代码执行漏洞	高	目前厂商已经发布了补丁修复程序，请广大用户及时下载：http://web.mit.edu/~kerberos/
CNVD-2015-00935	Cobham Sailor 900 VSAT 存在未明远程缓冲区溢出漏洞	高	否
CNVD-2015-00940	ArticleFR 'videouploader.php'任意文件上传漏洞	高	否

表 3 部分高危漏洞列表

小结：本周，Apple、IBM、Cisco 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、提升权限、执行任意代码或发起拒绝服务攻击；Google Chrome 存在内存错误引用、未授权访问和拒绝服务漏洞，允许攻击者利用漏洞发起拒绝服务攻击。此外，Microsoft Windows User Profile 被披露存在一个高危零日漏洞，攻击者可利用漏洞提升服务权限。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、Adobe 修补 Flash Player 产品漏洞

Adobe Flash Player 是一种广泛使用的、专有的多媒体程序播放器。

本周，Apache 修补了上述产品存在的双重释放远程代码执行等漏洞，避免攻击者利用漏洞在受影响应用程序上下文中执行任意代码，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/54934

http://www.cnvd.org.cn/patchInfo/show/54751

本周要闻速递

1. Google Play 商店出现恶意传播广告 APP 感染超过 1500 万用户

目前，安全专家已经在谷歌 Play 商店中发现了 3 个恶意安卓应用（APP），它们提供恶意广告下载服务。这三款恶意 APP 为：Durak 卡牌游戏、IQ Test、Russian History，是目前流行的游戏 APP，且都能在谷歌 Play 商店中免费下载，下载时可以很明显看出这些 APP 是由不同开发者发布的。根据下载量统计，单就卡牌游戏 Durak 就有 500 万到 1000 万的安装量，而这三款应用的总下载量已经超过了 1500 万次。一旦受害者在移动设备上安装了这些恶意应用，随着时间的推移，用户就能发现一些异常行为，并能察觉到设备的性能逐渐变得很差。

参考链接：http://www.freebuf.com/news/58513.html

2. iOS 版 Outlook 被披露存在多处安全隐患

前不久微软刚刚发布了 iOS 版 Outlook 应用程序，而这几天安全研究人员发现其数个安全隐患，包括微软可以在用户毫不知情的情况下获取用户的邮箱账户和服务器数据。目前，主要有云端存储用户登录信息、邮件管理混乱和云存储风险等安全隐患。安全研究人员称，苹果内置的托管和非托管应用程序是无法解决这一问题的，因为 Outlook 通信属于内部应用程序，用户无法控制它。因此，安全研究人员建议管理员通知所有的员工不要使用 iOS 版 Outlook 应用程序，并禁止该应用程序访问公司邮箱服务器。

参考链接：http://www.freebuf.com/news/58319.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