

信息安全漏洞周报

2015 年 07 月 27 日-2015 年 08 月 02 日

2015 年第 31 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 228 个，其中高危漏洞 58 个、中危漏洞 146 个、低危漏洞 24 个。上述漏洞中，可利用来实施远程攻击的漏洞有 207 个。本周收录的漏洞中，已有 211 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“WordPress wp-powerplaygallery 插件'upload.php'存在多个 SQL 注入漏洞”、“Microsoft Internet Explorer 'CTableLayout::AddRow()'越界内存破坏漏洞”等零日漏洞，请使用相关产品的用户注意加强防范。

本周，互联网上披露了涉及 Android 手机操作系统存在的彩信远程代码执行漏洞，根据 CNVD 测试结果，情况属实，通过远程攻击可向手机终端植入恶意程序。建议广大用户及时关注官方发布的补丁情况，同时不要接收不明来源的彩信信息并关闭手机的自动接收和打开彩信功能。

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 228 个漏洞。报送情况如表 1 所示。其中，奇虎、安天实验室、启明星辰、绿盟科技、天融信等单位报送数量较多。此外，CNCERT 各分中心、广州白狐网络科技有限公司、乌云、漏洞盒子、High-Tech Bridge Security Research Lab 及白帽子向 CNVD 提交了 665 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	291	291
安天实验室	234	0

启明星辰	72	0
绿盟科技	51	0
天融信	50	0
恒安嘉新	42	0
High-Tech Bridge Security Research Lab	1	1
乌云	303	303
漏洞盒子	50	50
广州白狐网络科技有限公司	1	1
CNCERT 新疆分中心	3	3
CNCERT 宁夏分中心	1	1
个人	15	15
报送总计	1114	665
录入总计	228（去重）	665

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、Google、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	Oracle	60	26%
2	Google	28	12%
3	Cisco	19	8%
4	WordPress	17	7%
5	IBM	7	3%
6	Drupal	6	3%
7	Microsoft	5	2%
8	Joomla!	5	2%
9	Moodle	4	2%

10	其他	77	35%
----	----	----	-----

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 228 个漏洞。其中应用程序漏洞 144 个，WEB 应用漏洞 34 个，操作系统漏洞 19 个，数据库漏洞 16 个，网络设备漏洞 13 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	144
WEB 应用漏洞	34
操作系统漏洞	19
数据库漏洞	16
网络设备漏洞	13
安全产品漏洞	2

表 3 漏洞按影响类型统计表

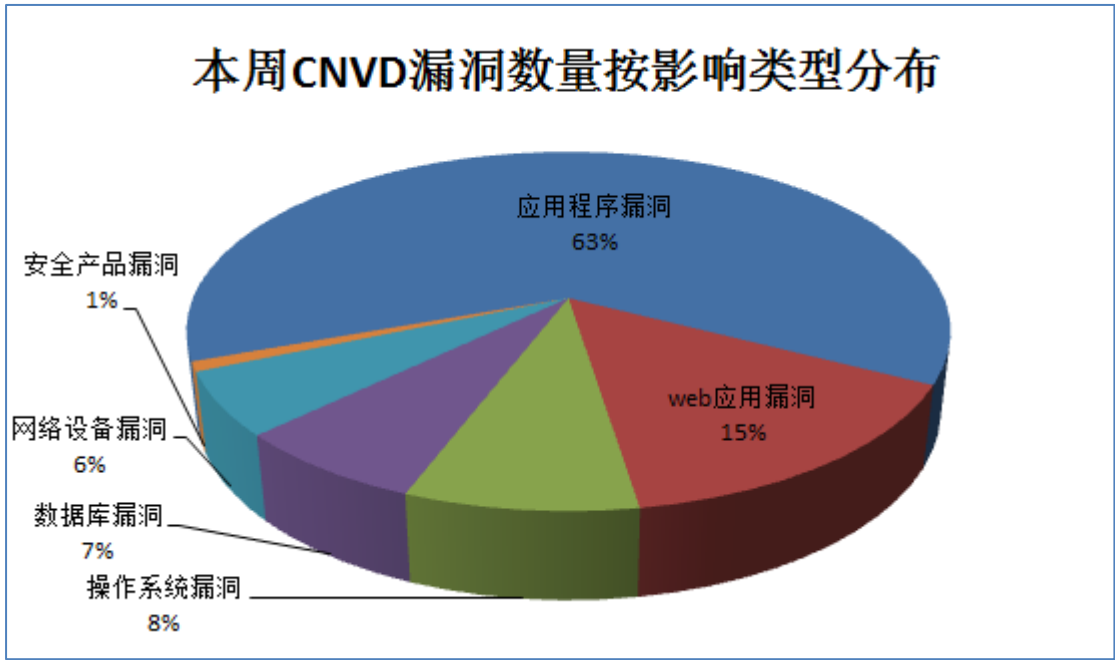


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 34 个电信行业漏洞，2 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，“Oracle Fusion Oracle Access Manager 组件存在未明漏洞（CNVD-2015-04875）、Cisco Application Policy Infrastructure Controllers 和 Nexus 9000 Series ACI Mode Switches 未授权访问漏洞、Belkin N300 Dual-Band Wi-Fi Range Extender 远程代码执行漏洞、Cisco IOS 和 IOS XE Software 拒绝服务漏洞（CN

VD-2015-04986)、BlackBerry Link Codec Demux MP4 处理任意代码执行漏洞、Siemens SICAM MIC 身份验证绕过漏洞”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	危险等级	是否有补丁
电信	CNVD-2015-04872	Oracle Fusion Oracle Access Manager 组件存在未明漏洞 (CNVD-2015-04872)	中	是
电信	CNVD-2015-04870	Oracle Fusion Web Cache 组件存在未明漏洞	中	是
电信	CNVD-2015-04871	Oracle Fusion Oracle GlassFish Server 组件存在未明漏洞 (CNVD-2015-04871)	中	是
电信	CNVD-2015-04868	Oracle Fusion Oracle Business Intelligence Enterprise Edition 组件存在未明漏洞	低	是
电信	CNVD-2015-04869	Oracle Fusion Oracle GlassFish Server 组件存在未明漏洞 (CNVD-2015-04869)	低	是
电信	CNVD-2015-04875	Oracle Fusion Oracle Access Manager 组件存在未明漏洞 (CNVD-2015-04875)	高	是
电信	CNVD-2015-04874	Oracle Fusion Oracle Event Processing 组件存在未明漏洞	中	是
电信	CNVD-2015-04873	Oracle Fusion Oracle JDeveloper 组件存在未明漏洞	中	是
电信	CNVD-2015-04889	Oracle MySQL client 组件存在未明漏洞	低	是
电信	CNVD-2015-04907	Oracle MySQL Server:DML 组件存在未明漏洞 (CNVD-2015-04907)	中	是
电信	CNVD-2015-04892	Oracle MySQL Server:PluggableAuth 组件存在未明漏洞	低	是
电信	CNVD-2015-04914	Oracle MySQL Server:RBR 组件存在未明漏洞	低	是
电信	CNVD-2015-04908	Oracle MySQL Server:DML 组件存在未明漏洞 (CNVD-2015-04908)	中	是
电信	CNVD-2015-04911	Oracle MySQL Server:Optimizer 组件存在未明漏洞 (CNVD-2015-04911)	中	是
电信	CNVD-2015-04913	Oracle MySQL Server:Partition 组件存在未明漏洞	中	是
电信	CNVD-2015-04909	Oracle MySQL Server:Memcached 组件存在未明漏洞	低	是
电信	CNVD-2015-04910	Oracle MySQL Server:Optimizer 组件存在未明漏洞 (CNVD-2015-04910)	低	是
电信	CNVD-2015-04912	Oracle MySQL Server:Partition 组件存在未明漏洞 (CNVD-2015-04912)	中	是
电信	CNVD-2015-04930	Oracle MySQL Server:I_S 组件存在未明漏洞	中	是

电信	CNVD-2015-04931	Oracle MySQL Server:InnoDB 组件存在未明漏洞	中	是
电信	CNVD-2015-04956	Juniper Junos IPv6 SEND 处理拒绝服务漏洞	中	是
电信	CNVD-2015-04949	Juniper Junos 拒绝服务漏洞 (CNVD-2015-04949)	中	是
电信	CNVD-2015-04950	Juniper Networks Junos SRX Series SRX Network Security Daemon 拒绝服务漏洞	中	是
电信	CNVD-2015-04959	Cisco ASR 5000 Router GTPv2 输入验证拒绝服务漏洞	中	是
电信	CNVD-2015-04962	Cisco Prime Collaboration Assurance Web 接口拒绝服务漏洞	中	是
电信	CNVD-2015-04965	Cisco WebEx Meetings Server 验证用户任意代码执行漏洞	中	是
电信	CNVD-2015-04969	Fiat Chrysler Automobiles Uconnect 远程权限提升漏洞	高	否
电信	CNVD-2015-04981	Cisco Application Policy Infrastructure Controllers 和 Nexus 9000 Series ACI Mode Switches 未授权访问漏洞	高	是
电信	CNVD-2015-04993	Belkin N300 Dual-Band Wi-Fi Range Extender 远程代码执行漏洞	高	是
电信	CNVD-2015-04995	Cisco IOS XR for ASR 9000 Series Router 报文处理目标 BGP 服务拒绝漏洞	中	是
电信	CNVD-2015-04986	Cisco IOS 和 IOS XE Software 拒绝服务漏洞 (CNVD-2015-04986)	高	是
电信	CNVD-2015-04988	Cisco WebEx Meetings Server 跨站请求伪造漏洞 (CNVD-2015-04988)	中	是
电信	CNVD-2015-05037	Cisco ASR9k IOS XR Local Packet Transport Services 拒绝服务漏洞	中	是
电信	CNVD-2015-05041	Cisco AnyConnect Secure Mobility Client 拒绝服务漏洞	中	是
移动互联网	CNVD-2015-04932	BlackBerry Link Codec Demux MP4 处理任意代码执行漏洞	高	是
移动互联网	CNVD-2015-04978	Android 系统备份后还原处理上恶意 APK 注入漏洞	中	否
工控系统	CNVD-2015-04832	Siemens SICAM MIC 身份验证绕过漏洞	高	是
工控系统	CNVD-2015-04982	Siemens SIMATIC WinCCSm@rtClient for Android 密码信息泄露漏洞	低	是

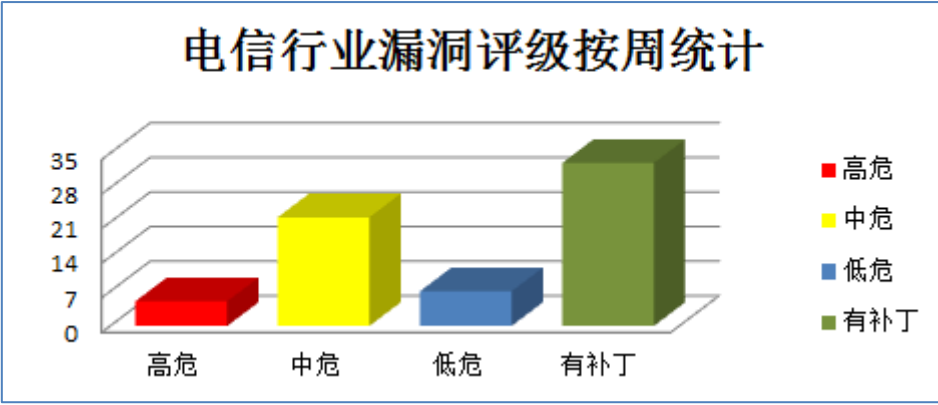


图 1 电信行业漏洞统计

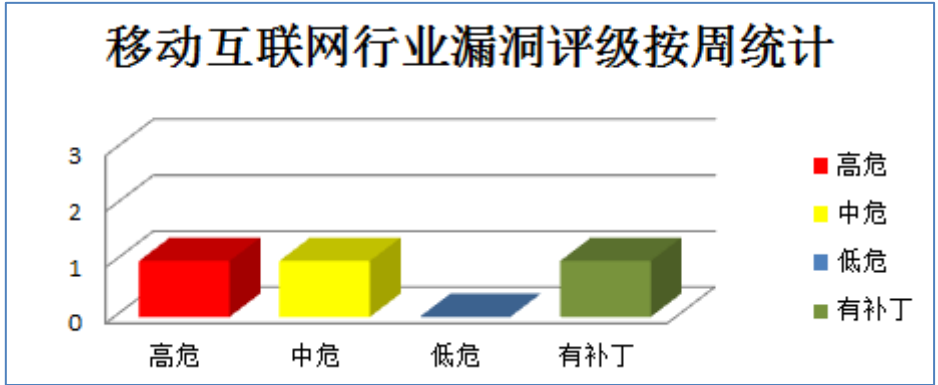


图 2 移动互联网行业漏洞统计

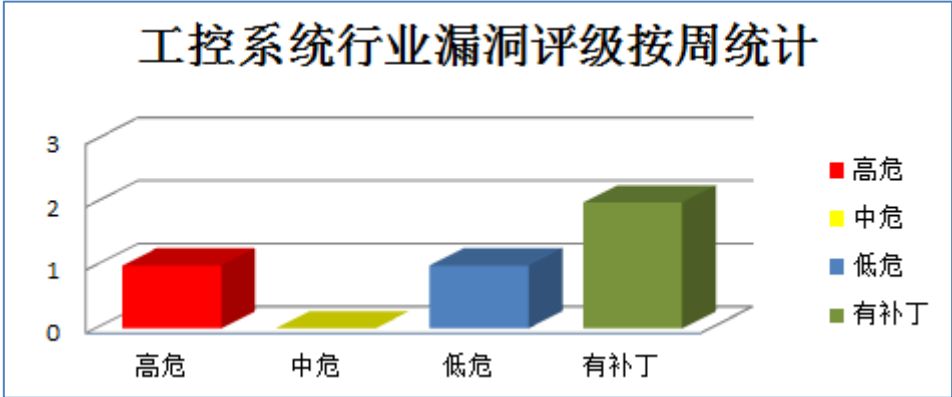


图 3 工控系统行业漏洞统计

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、ISC 产品安全漏洞

本周，CNVD 收录了一个 ISC BIND 9 TKEY 查询拒绝服务漏洞(CNVD-2015-05040，对应 CVE-2015-5477)。远程攻击者可通过 TKEY 查询，导致拒绝服务。

CNVD 收录的相关漏洞包括：ISC BIND 9 TKEY 查询拒绝服务漏洞。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-2015-05040>

2、Oracle 产品安全漏洞

Oracle MySQL Server 是一款关系型流行的数据库。本周，上述产品被披露存在未明漏洞。攻击者利用漏洞可影响系统保密性、完整性和可用性。

CNVD 收录的相关漏洞包括：Oracle MySQL Server:Partition 组件存在未明漏洞（CNVD-2015-04913）、Oracle MySQL Server:Memcached 组件存在未明漏洞、Oracle MySQL Server:Optimizer 组件存在未明漏洞（CNVD-2015-04910）、Oracle MySQL Server:Partition 组件存在未明漏洞、Oracle MySQL Server:RBR 组件存在未明漏洞、Oracle MySQL client 组件存在未明漏洞、Oracle MySQL Server:DML 组件存在未明漏洞（CNVD-2015-04908）、Oracle MySQL Server:I_S 组件存在未明漏洞。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-2015-04913>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04909>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04910>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04912>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04914>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04889>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04908>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04930>

3、Google 产品安全漏洞

Stagefright 是适用于 Android 的媒体播放服务，自 2.2 (Froyo)版本开始引入。Google Chrome 是一款开源的 WEB 浏览器。本周，上述产品被披露存在远程任意代码执行和内存错误引用漏洞。攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Google Stagefright Media Playback Engine 远程代码执行漏洞（CNVD-2015-05030、CNVD-2015-05029、CNVD-2015-05028、CNVD-2015-05027、CNVD-2015-05026、CNVD-2015-05025、CNVD-2015-05024）、Google Chrome GPU 处理实现内存错误引用漏洞。其中，除“Google Chrome GPU 处理实现内存错误引用漏洞”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-2015-05030>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05029>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05028>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05027>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05026>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05025>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05024>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04898>

4、Microsoft 产品安全漏洞

Internet Explorer 是微软公司推出的一款网页浏览器。Microsoft windows 是一款流行的操作系统。Microsoft Malicious Software Removal Tool 是其系统上的一款恶意软件删除工具。本周，上述产品被披露存在远程代码执行、内存破坏和权限提升漏洞。攻击者可利用漏洞执行任意代码或提升权限。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer CAttrArray 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer CCurrentStyle 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer CTreePos 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer 'CTableLayout::AddRow()'越界内存破坏漏洞、Microsoft 恶意软件删除工具 DLL 加载本地权限提升漏洞。其中，“Microsoft Internet Explorer 'CTableLayout::AddRow()'越界内存破坏漏洞、Microsoft 恶意软件删除工具 DLL 加载本地权限提升漏洞”的综合评级为“高危”。目前，厂商已经发布了“Microsoft 恶意软件删除工具 DLL 加载本地权限提升漏洞”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-2015-05010>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05012>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-05011>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04984>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-04954>

5、Fiat Chrysler Automobiles Uconnect 远程权限提升漏洞

Fiat Chrysler Automobiles Uconnect 是美国菲亚特克莱斯勒汽车（Fiat Chrysler Automobiles, FCA）公司的一套车载信息系统。本周，Fiat Chrysler Automobiles Uconnect 被披露存在综合评级为“高危”的权限提升漏洞。攻击者利用该漏洞可控制车辆移动，造成人类伤害或物理伤害，或修改仪表盘设置。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-2015-04969>

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-2015-04890	多个 Panda 安全产品'PSKMAD.sys'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： http://www.pandasecurity.com/usa/
CNVD-2015-04929	RubyGems ruby-saml‘xml_security.rb’命令注入漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://rubygems.org/gems/ruby-saml/versions/
CNVD-2015-04932	BlackBerry Link Codec Demux MP4 处理任意代码执行漏洞	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://www.blackberry.com/btsc/KB37207
CNVD-2015-04938	Elasticsearch 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此安全问题，补丁获取链接： https://www.elastic.co/community/security
CNVD-2015-04968	WordPress Easy2Map Photos 插件 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： https://wordpress.org/plugins/easy2map-photos/
CNVD-2015-04977	Eaton Cooper Power Systems ProView 中间人攻击漏洞	高	用户可联系供应商获得补丁信息： http://www.eaton.com
CNVD-2015-04980	GemaltoSafeNet Luna HSM 存在未明漏洞	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://www.safenet-inc.com/technical-support/security-updates/
CNVD-2015-04989	TIBCO Spotfire Analyst 存在多个未明漏洞	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://www.tibco.com/mk/advisory.jsp
CNVD-2015-04993	Belkin N300 Dual-Band Wi-Fi Range Extender 远程代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://www.belkin.com/us/support-article?articleNum=4975
CNVD-2015-04998	PHP ‘phar_fix_filepath()’函数栈缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://bugs.php.net/bug.php?id=69923

表 3 部分高危漏洞列表

小结：本周，CNVD 收录了一个 ISC BIND 9 TKEY 查询拒绝服务漏洞（CNVD-2015-05040，对应 CVE-2015-5477）。远程攻击者可通过 TKEY 查询，导致拒绝服务。此外，Oracle 多款产品被披露存在多个安全漏洞，攻击者利用漏洞可影响系统完整性、保密性和可用性。Google、Microsoft 多款产品被披露存在多个安全漏洞，攻击者利用漏洞

行任意代码或提升权限。另外，Fiat Chrysler Automobiles Uconnect 被披露存在一个高危零日漏洞，攻击者利用该漏洞可控制车辆移动，造成人类伤害或物理伤害，或修改仪表盘设置。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、QEMU 修补 QEMU 产品漏洞

QEMU 是法国程序员法布里斯-贝拉（FabriceBellard）所研发的一套模拟处理器软件。该软件具有速度快、跨平台等特点。

本周，QEMU 修补了上述产品存在的拒绝服务漏洞，避免攻击者利用漏洞发起拒绝服务攻击。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/61769>

本周要闻速递

1. 安卓再曝新漏洞：可远程致使用户无法接打电话

安全研究员在安卓设备的 mediaserver 服务上发现了一个整数溢出漏洞。mediaserver 服务是安卓手机用于索引媒体文件的一个服务。造成该安全威胁的原因是 mediaserver 服务不能正确的处理畸形文件。当 mediaserver 服务解析 MKV 文件时会出现整数溢出，解析音频数据时，攻击者可以读取缓冲区数据，重写 NULL 数据。所以会导致服务崩溃。Android 4.3 Jelly Bean 及其之后的所有版本均受影响，包括 Android 5.1.1 Lollipop，以至于有数百万的安卓用户都可能被黑客攻击。

参考链接：<http://www.freebuf.com/news/73755.html>

2. 苹果 App Store 和 iTunes Store 曝高危漏洞

漏洞实验室（Vulnerability-Lab）创始人兼安全研究员 Benjamin Kunz Mejri 在苹果 App Store 购买清单模块中发现了一个应用程序端输入验证 web 漏洞。远程攻击者可以利用该漏洞将设备的名称字段替换成一个恶意脚本代码，从而操纵设备的名称字段。如果攻击者在 App Store 和 iTunes Store 中购买产品，内部应用程序服务就会利用设备名称字段（实际上是恶意代码），然后生成一个购买清单发给卖方账户。

参考链接：<http://www.freebuf.com/news/73570.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