

## 信息安全漏洞周报

2012 年 9 月 24 日-2012 年 9 月 30 日

2012 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 155 个，其中高危漏洞 57 个、中危漏洞 86 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 145 个。本周收录的漏洞中，已有 102 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“QNX Qconn 远程任意命令执行漏洞”、“ViArt Shop Enterprise 'sips\_response.php'任意命令执行漏洞”等的零日攻击代码，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 8 家成员单位和多个合作伙伴报送了本周收录的全部 155 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技、安天实验室等单位报送数量较多。此外，网御星云公司以及个人漏洞研究者向 CNVD 提交了 2 个原创漏洞。

| 报送单位或个人 | 漏洞报送数量 | 原创漏洞数量 |
|---------|--------|--------|
| 绿盟科技    | 119    | 0      |
| 启明星辰    | 173    | 0      |
| 安天实验室   | 80     | 0      |
| 恒安嘉新    | 42     | 0      |
| 天融信     | 56     | 0      |
| 安氏领信    | 12     | 0      |
| 东软      | 3      | 0      |
| 知道创宇    | 2      | 0      |
| 网御星云    | 1      | 1      |
| 个人报送者   | 1      | 1      |

|      |         |   |
|------|---------|---|
| 报送总计 | 489     | 2 |
| 录入总计 | 155（去重） | 2 |

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Google、IBM、WordPress、Cisco 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  | Google    | 24   | 15%  |
| 2  | IBM       | 12   | 8%   |
| 3  | WordPress | 10   | 6%   |
| 4  | Cisco     | 9    | 6%   |
| 5  | HP        | 7    | 5%   |
| 6  | Novell    | 4    | 3%   |
| 7  | Microsoft | 4    | 3%   |
| 8  | Gwebmail  | 3    | 1%   |
| 9  | Oracle    | 2    | 1%   |
| 10 | Linux     | 1    | 1%   |
| 11 | 其它        | 79   | 51%  |

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 155 个漏洞。其中操作系统漏洞 2 个，应用程序漏洞 103 个，WEB 应用漏洞 36 个，网络设备漏洞 11 个，数据库漏洞 2 个，安全产品漏洞 1 个。

| 漏洞影响对象类型 | 漏洞数量 |
|----------|------|
| 操作系统漏洞   | 2    |
| 应用程序漏洞   | 103  |
| WEB 应用漏洞 | 36   |
| 网络设备漏洞   | 11   |
| 安全产品漏洞   | 1    |
| 数据库漏洞    | 2    |

表 3 漏洞按影响类型统计表

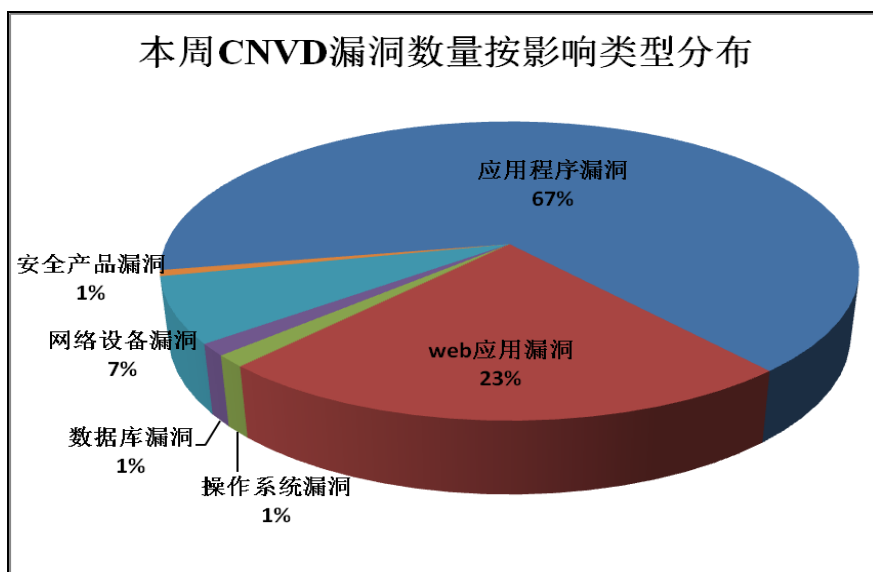


图 1 本周漏洞按影响类型分布

### 本周涉及电信行业漏洞信息

本周，CNVD 收录了 11 个网络设备漏洞：WAN Emulator result.php pc 参数任意命令执行漏洞、Cisco IOS/Unified Communications Manager 拒绝服务漏洞、Cisco IOS 远程拒绝服务漏洞（CNVD-2012-14834）、Cisco IOS 格式不正确属性远程拒绝服务漏洞、Cisco IOS DHCP 服务器拒绝服务漏洞、Cisco IOS DHCP Version 6 服务器拒绝服务漏洞、Cisco IOS NAT 功能远程拒绝服务漏洞（CNVD-2012-14843）、Cisco IOS NAT 功能远程拒绝服务漏洞（CNVD-2012-14844）、Cisco IOS Queue Wedge 拒绝服务漏洞（CNVD-2012-14845）、Samsung Galaxy S III USSD 代码远程拒绝服务漏洞、Cisco Catalyst 4500E 系列交换机拒绝服务漏洞。其中，除“Samsung Galaxy S III USSD 代码远程拒绝服务漏洞”和“WAN Emulator result.php pc 参数任意命令执行漏洞”外，其余漏洞的综合评级均为“高危”。目前，相关生产厂商尚未提供完整的修复方案，请相关用户关注厂商主页以及及时获取安全更新。

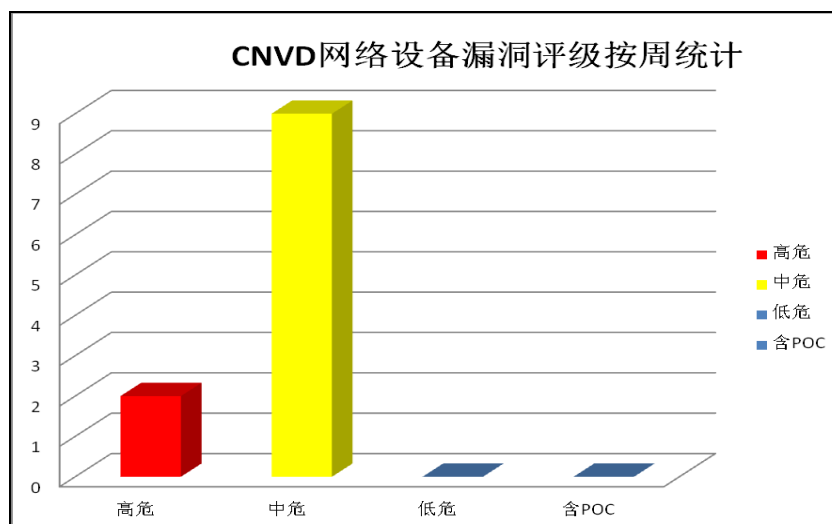


图 2 网络设备漏洞统计

## 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、Google Chrome 安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome SSE2 优化缓冲区溢出漏洞（CNVD-2012-14805）、Google Chrome 插件处理内存错误引用漏洞（CNVD-2012-14810）、Google Chrome onclick 处理内存错误引用漏洞、Google Chrome SVG 文本引用内存错误引用漏洞、Google Chrome WebGL 整数溢出漏洞、Google Chrome 插件 DOM 树破坏漏洞、Google Chrome 插件绘图缓冲漏洞（CNVD-2012-14816）、Google Chrome Skia 越界写漏洞（CNVD-2012-14823）等。上述漏洞的综合评级均为“高危”。厂商已经修复了上述漏洞，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/sites/main/preview/ldgg\\_preview.htm?tid=58342](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58342)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58347](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58347)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58356](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58356)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58357](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58357)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58370](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58370)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58361](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58361)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58358](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58358)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58365](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58365)

## 2、IBM 产品安全漏洞

IBM WebSphere MQ 是一款用于面向企业级应用提供信息传输服务的解决方案；IBM WebSphere Application Server (WAS) 是一种由 IBM 开发并发行的应用服务器；IBM WebSphere Commerce 是一款商务应用开发软件；IBM Informix Dynamic Server 是一款动态数据库管理软件；IBM DB2 是一款大型的商业关系数据库系统。本周，上述 IBM 产品被披露存在多个安全漏洞，攻击者利用漏洞可劫持会话，发起拒绝服务攻击，或以数据库服务器的权限执行任意代码，修改或删除系统上的文件。

CNVD 收录的相关漏洞包括：IBM WebSphere MQ Server Message Channel Agent 拒绝服务漏洞、IBM WebSphere Application Server 验证缓存数据清除漏洞、IBM WebSphere Application Server 文件目录遍历漏洞、IBM WebSphere Commerce 拒绝服务漏洞、IBM WebSphere Application Server ISC 控制台会话劫持漏洞、IBM Informix Dynamic Server 缓冲区溢出漏洞（CNVD-2012-14782）、IBM WebSphere Commerce 存在多个漏洞、IBM DB2 UTL\_FILE 模块目录遍历漏洞等。其中，“IBM Informix Dynamic Server 缓冲区溢出漏洞（CNVD-2012-14782）、IBM WebSphere Commerce 存在多个漏洞、IBM DB2 UTL\_FILE 模块目录遍历漏洞”的综合评级均为“高危”。目前，厂商已经修复了上述漏洞。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/sites/main/preview/ldgg\\_preview.htm?tid=58315](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58315)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58333](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58333)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58331](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58331)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58330](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58330)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58327](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58327)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58319](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58319)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58328](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58328)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58336](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58336)

## 3、HP 产品安全漏洞

HP SiteScope 是一款提供 IT 基础设施的可用性和性能监测服务的解决方案；HP Network Node Manager i 是一款网络服务智能插件 (iSPI)，用于进一步扩展现有软件的可用性功能。本周，上述 HP 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或劫持用户会话，执行任意代码。

CNVD 收录的相关漏洞包括：HP SiteScope soap 任意代码执行漏洞（CNVD-2012-14808、CNVD-2012-14809、CNVD-2012-14806、CNVD-2012-14811、CNVD-2012-14812、CNVD-2012-14803）、HP Network Node Manager i 跨站脚本漏洞（CNVD-2012-14744）。其中，除“HP Network Node Manager i 跨站脚本漏洞（CNVD-2012-14744）”外，其余漏洞的综合评级均为“高危”。目前，厂商已经发布了安全公告，修复了除“HP N

etwork Node Manager i 跨站脚本漏洞（CNVD-2012-14744）”外的其余漏洞。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/sites/main/preview/ldgg\\_preview.htm?tid=58345](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58345)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58346](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58346)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58348](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58348)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58348](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58348)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58349](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58349)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58340](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58340)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58208](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58208)

4、Microsoft 产品安全漏洞

Microsoft Internet Explorer 是一款流行的 WEB 浏览器。本周，该产品被披露存在多个漏洞，远程攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer OnMove 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer Event Listener 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer Layout 内存错误引用远程代码执行漏洞、Microsoft Internet Explorer cloneNode 内存错误引用远程代码执行漏洞。目前，厂商已经发布补丁信息修复上述 IE 漏洞。CNVD 提醒广大用户及时下载补丁更新。

参考链接：[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58199](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58199)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58201](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58201)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58200](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58200)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=58202](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58202)

5、ViArt Shop Enterprise 'sips\_response.php'任意命令执行漏洞

ViArt Shop Enterprise 是一款应用较为广泛的网上商店系统建站软件。本周，ViArt Shop Enterprise 被披露存在一个综合评级为“高危”的任意命令执行漏洞。ViArt Shop Enterprise 'sips\_response.php'未能正确过滤用户提交的请求，攻击者利用漏洞以 WEB 权限执行任意系统命令。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/sites/main/preview/ldgg\\_preview.htm?tid=58329](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=58329)

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/publish/main/52/index.html>

| CNVD 编号         | 漏洞名称                   | 综合<br>评级 | 修复方式 |
|-----------------|------------------------|----------|------|
| CNVD-2012-14841 | YingZhiPython 任意文件上传漏洞 | 高        | 暂无   |

|                 |                                                 |   |                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|-------------------------------------------------|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CNVD-2012-14833 | Cisco IOS/Unified Communications Manager 拒绝服务漏洞 | 高 | 用户可参考如下供应商提供的安全公告获得补丁信息：<br><a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-sip</a><br><a href="http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-cucm">http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20120926-cucm</a> |
| CNVD-2012-14795 | QNX Qconn 远程任意命令执行漏洞                            | 高 | 暂无                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| CNVD-2012-14838 | Foxit Reader 'fxdecod1.dll' DLL 装载任意代码执行漏洞      | 高 | Foxit Reader 5.4.3 已经修复此漏洞，建议用户下载使用：<br><a href="http://www.foxitsoftware.com/">http://www.foxitsoftware.com/</a>                                                                                                                                                                                                                                                                                                                        |
| CNVD-2012-14787 | LibTIFF TIFF 图像堆缓冲区溢出漏洞                         | 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：<br><a href="http://www.libtiff.org">http://www.libtiff.org</a>                                                                                                                                                                                                                                                                                                                                         |
| CNVD-2012-14800 | Mcafee Email Anti-virus 拒绝服务漏洞                  | 高 | 暂无                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| CNVD-2012-14785 | phpMyAdmin Compromised Source Package 后门漏洞      | 高 | 用户可参考如下供应商提供的安全公告获得补丁信息：<br><a href="http://www.phpmyadmin.net/home_page/security/PMASA-2012-5.php">http://www.phpmyadmin.net/home_page/security/PMASA-2012-5.php</a>                                                                                                                                                                                                                                                                    |
| CNVD-2012-14784 | Simple PHP Forum SQL 注入漏洞                       | 高 | 暂无                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| CNVD-2012-14718 | Red Hat Enterprise MRG Grid SQL 注入漏洞            | 高 | 用户可参考如下 SVN 库获得相关的补丁信息：<br><a href="http://svn.fedorahosted.org/svn/cumin">http://svn.fedorahosted.org/svn/cumin</a>                                                                                                                                                                                                                                                                                                                     |
| CNVD-2012-14706 | Apple Mac OS X DirectoryService 服务缓冲区溢出漏洞       | 高 | 用户可参考如下供应商提供的安全公告获得补丁信息：<br><a href="http://support.apple.com/kb/HT5501">http://support.apple.com/kb/HT5501</a>                                                                                                                                                                                                                                                                                                                          |
| CNVD-2012-14698 | GOM Player 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此安全问题，补丁获取链接：<br><a href="http://player.gomlab.com/eng/notice/view.gom?intseq=147">http://player.gomlab.com/eng/notice/view.gom?intseq=147</a>                                                                                                                                                                                                                                                                           |

表 3 部分高危漏洞列表

本周，Google Chrome 和 Microsoft Internet Explorer 浏览器被披露存在多个安全漏洞，攻击者利用漏洞可执行任意代码，有可能发起大规模挂马攻击，请广大浏览器用户安装主机防护软件加强防范。HP、IBM 的多款产品也被披露存在多个安全漏洞，攻击者利用漏洞可劫持会话，发起拒绝服务攻击，或进行未经授权修改。上述产品由于应用广泛且与企业、个人信息数据关联度高，需引起企业用户和管理员用户高度重视。此外，

ViArt Shop Enterprise 网上商店建站软件被披露存在零日漏洞，建议采用该软件的电商用户随时关注厂商主页，以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 布升级程序，修补 Kernel 漏洞

Linux 是一款开源的操作系统。本周，Linux 修补了 Kernel 存在的漏洞。攻击者可以利用漏洞导致系统崩溃。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/sites/main/preview/bdgg\\_preview.htm?tid=23265](http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=23265)

## 本周要闻速递

### 1. Java 新漏洞致 10 亿电脑处于安全威胁中

甲骨文 Java 软件中发现了最新的 0day 漏洞，这一漏洞几乎出现在所有受支持的 Java 版本中，通过此漏洞，黑客可在超过 10 亿台装有 Java 的 Mac 和 PC 机上安装恶意软件与病毒。这一安全漏洞存在于 Java 5、Java 6 和 Java 7 中。计算机世界还特别指出，使用 Mac OS X 最新版本系统的用户同样存在这一安全问题，包括 Snow Leopard 10.6 系统。10 亿这一数据是甲骨文根据已安装的计算机数目进行统计得出的。关于这一漏洞的技术细节目前还没有完全公开，据说甲骨文正着手为修复此问题发布补丁，但没有透露发布的具体时间，也不确定在 10 月 16 日 Java 的常规升级之前补丁能否完成。

参考链接：<http://networking.ctocio.com.cn/122/12439622.shtml>

### 2. iOS 6 的群组交流功能存在重大漏洞

iOS 6 位于 iCloud 功能下方的“微软交流群组”功能（Microsoft Exchange），这一类似于“收件箱”的功能被 iOS 6 的企业用户发现有“难以忽视”的漏洞。据 MacRumors 报道，已经有财富 500 强的企业要求他们的员工暂时不要升级 iOS 6 系统，原因是：当个人用户婉拒某一个会议的邀请时，系统会自动向会议所有的出席成员发送一个“会议取消”通知，而不是只向会议的组织者发送一个无法出席的情况说明。企业用户告知其内部员工们：在这一问题修复之前，暂时不要接受或拒绝任何日历议程的“邀请”。据悉，苹果和微软都已经发现该问题的存在，但双方暂未对此作出官方回应。

参考链接：[http://tech.ifeng.com/apple/news/detail\\_2012\\_10/04/18046989\\_0.shtml](http://tech.ifeng.com/apple/news/detail_2012_10/04/18046989_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的全称是国家计算机网络应急技术处理协调中心（英文简称是 CNCERT 或 CNCERT/CC）成立于 1999 年 9 月，是工业和信息化部领导下的国家级网络安全应急机构，致力于建设国家级的网络安全监测中心、预警中心和应急中心，以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能，支持基础信息网络的安全防护和安全运行，支援重要信息系统的网络安全监测、预警和处置；国家互联网应急中心在我国大陆 31 个省、自治区、直辖市设有分中心。

网址：[www.cert.org.cn](http://www.cert.org.cn)

邮箱：[vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话：010-82990999