

## 信息安全漏洞周报

2012 年 9 月 17 日-2012 年 9 月 23 日

2012 年第 38 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**高**。

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 207 个，其中高危漏洞 66 个、中危漏洞 128 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 188 个。本周收录的漏洞中，已有 144 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“VBulletin 'blog\_plugin\_useradmin.php' SQL 注入漏洞”、“NCMedia Sound Editor Pro 'MRUList201202.dat'文件栈缓冲区溢出漏洞”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 7 家成员单位和多个合作伙伴报送了本周收录的全部 207 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。

| 报送单位或个人 | 漏洞报送数量  | 原创漏洞数量 |
|---------|---------|--------|
| 绿盟科技    | 152     | 0      |
| 启明星辰    | 173     | 0      |
| 安天实验室   | 75      | 0      |
| 恒安嘉新    | 14      | 0      |
| 天融信     | 11      | 0      |
| 安氏领信    | 13      | 0      |
| 东软      | 6       | 0      |
| 报送总计    | 444     | 0      |
| 录入总计    | 207（去重） | 0      |

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、Drupal、Cisco、Red Hat 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     | 61   | 29%  |
| 2  | Drupal    | 19   | 9%   |
| 3  | Cisco     | 17   | 8%   |
| 4  | Red Hat   | 7    | 3%   |
| 5  | Moodle    | 5    | 2%   |
| 6  | Condor    | 4    | 2%   |
| 7  | LuxSoft   | 4    | 2%   |
| 8  | Debian    | 3    | 2%   |
| 9  | Microsoft | 2    | 1%   |
| 10 | McAfee    | 1    | 1%   |
| 11 | 其它        | 84   | 41%  |

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 207 个漏洞。其中操作系统漏洞 34 个，应用程序漏洞 109 个，WEB 应用漏洞 50 个，网络设备漏洞 10 个，安全产品漏洞 4 个。

| 漏洞影响对象类型 | 漏洞数量 |
|----------|------|
| 操作系统漏洞   | 34   |
| 应用程序漏洞   | 109  |
| WEB 应用漏洞 | 50   |
| 网络设备漏洞   | 10   |
| 安全产品漏洞   | 4    |
| 数据库漏洞    | 0    |

表 3 漏洞按影响类型统计表

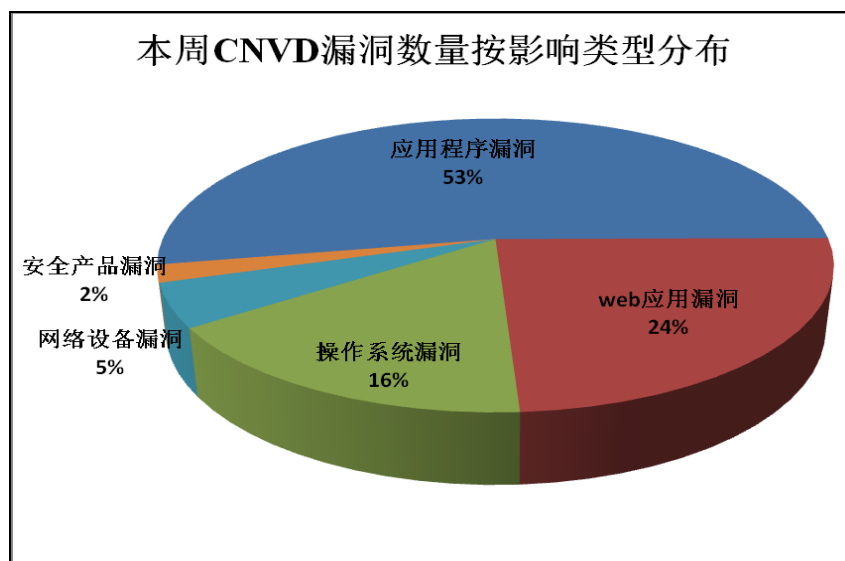


图 1 本周漏洞按影响类型分布

### 本周涉及电信行业漏洞信息

本周，CNVD 收录了 10 个网络设备漏洞：深信服应用交付管理系统文件包含漏洞、Cisco IOS 存在多个 IPv6 邻居拒绝服务漏洞（CNVD-2012-14585）、Cisco IOS FlexVPN 拒绝服务漏洞（CNVD-2012-14586）、Cisco IOS MVPNV6 更新拒绝服务漏洞（CNVD-2012-14587）、Cisco IOS DMVPN 通道实现拒绝服务漏洞（CNVD-2012-14588）、Cisco IOS SSL VPN 实现拒绝服务漏洞（CNVD-2012-14589）、Cisco IOS SSL VPN 实现拒绝服务漏洞（CNVD-2012-14591）、Cisco NX-OS ARP 报文拒绝服务漏洞、Technicolor THOMSON TWG850-4 HTTP 验证绕过漏洞、Microsoft Windows Phone 7 SSL 证书'Common Name'校验安全绕过漏洞。其中，“深信服应用交付管理系统文件包含漏洞”的综合评级为“高危”，生产厂商正在组织提供修复方案。

此外，互联网上已经出现了针对“Technicolor THOMSON TWG850-4 HTTP 验证绕过漏洞”和“Microsoft Windows Phone 7 SSL 证书'Common Name'校验安全绕过漏洞”的攻击代码。

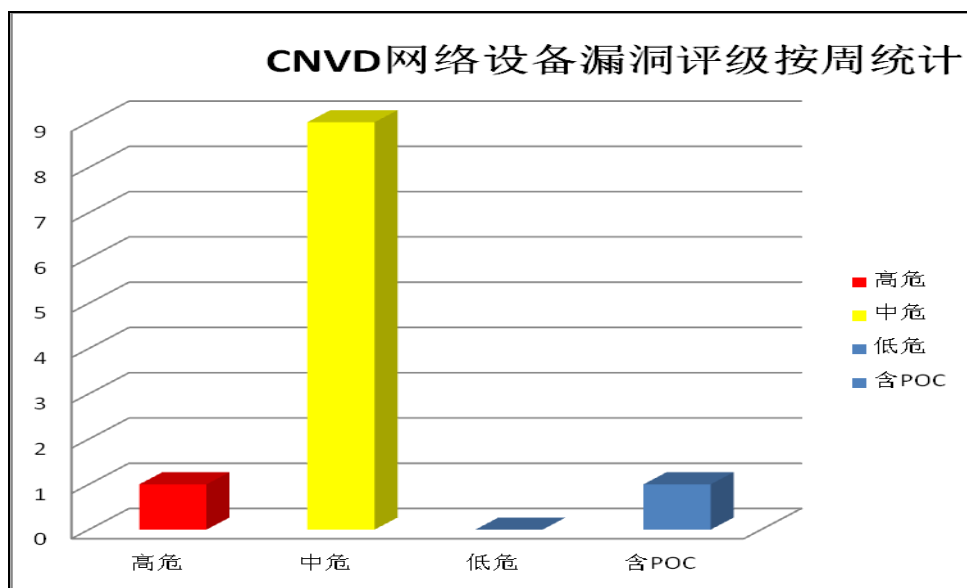


图 2 网络设备漏洞统计

## 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、Apple 产品安全漏洞

Apple iOS 是一款运行在苹果 iPhone 和 iPad/iPod touch 设备上的操作系统；WebKit 是一款开放源代码的浏览器引擎。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可伪造 SMS 消息返回地址，假冒任意用户发送 SMS 消息；构建恶意 WEB 站点，诱使应用程序解析，执行任意代码或使应用程序崩溃。

CNVD 收录的相关漏洞包括：Apple iPhone/iPad/iPod touch racoon 配置文件漏洞、Apple iPhone/iPad/iPod touch WebKit 内存破坏漏洞（CNVD-2012-14686）、Apple iPhone/iPad/iPod touch 短消息伪造漏洞（CNVD-2012-14690）、Apple iTunes 内存破坏漏洞（CNVD-2012-14559、CNVD-2012-14531、CNVD-2012-14530、CNVD-2012-14557、CNVD-2012-14552、）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=57821](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57821)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57866](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57866)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57870](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57870)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57306](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57306)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57259](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57259)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57258](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57258)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57304](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57304)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57299](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57299)

## 2、Drupal 模块安全漏洞

Drupal 是一款开源的网站内容管理系统（CMS）。本周，该产品的多个模块被披露存在多个安全漏洞，攻击者利用漏洞可获得数据库信息或劫持用户会话。

CNVD 收录的相关漏洞包括：Drupal Password Policy 模块跨站脚本漏洞、Drupal Password Policy 模块跨站请求伪造漏洞、Drupal Webform 模块 HTML 注入漏洞、Drupal Read More Link 跨站脚本漏洞、Drupal Multisite Search 模块 SQL 注入漏洞、Drupal Block Class 模块跨站脚本漏洞、Drupal Admin tools 模块跨站脚本漏洞、Drupal Admin tools 模块跨站请求伪造漏洞等。其中，“Drupal Multisite Search 模块 SQL 注入漏洞”的综合评级为“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=57863](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57863)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57862](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57862)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57755](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57755)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57635](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57635)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57595](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57595)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57515](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57515)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57500](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57500)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57499](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57499)

## 3、Cisco 产品安全漏洞

Cisco Intrusion Prevention System (IPS)是一款入侵防御系统应用平台；Cisco IOS 是思科网络产品使用的一款 Internet 操作系统；Cisco Nexus 系列交换机是数据中心级交换机；Cisco Secure Desktop 是一款用户桌面安全管理软件。本周，上述 Cisco 产品被披露存在多个安全漏洞，攻击者利用漏洞可构建恶意 WEB 页，诱使应用程序执行 ActiveX 控件或 Java Applet，执行任意代码；使进程崩溃或者通信中断，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Secure Desktop 任意代码执行漏洞（CNVD-2012-14684）、Cisco IPS sensorApp 内存破坏漏洞（CNVD-2012-14593）、Cisco IOS Flex VPN 拒绝服务漏洞（CNVD-2012-14586）、Cisco IOS 存在多个 IPv6 邻居拒绝服务漏洞（CNVD-2012-14585）、Cisco IOS DMVPN 通道实现拒绝服务漏洞（CNVD-2012-14588）、Cisco IOS SSL VPN 实现拒绝服务漏洞（CNVD-2012-14589）、Cisco Unity ConnectionUDP 拒绝服务漏洞（CNVD-2012-14600）、Cisco NX-OS ARP 报文拒绝服务漏洞等。其中，“Cisco Secure Desktop 任意代码执行漏洞（CNVD-2012-14684）”和“Cisco IPS sensorApp 内存破坏漏洞（CNVD-2012-14593）”的综合评级均为“高危”。目前，厂商已经发布了安全公告，修复了上述漏洞。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=57864](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57864)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57425](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57425)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57417](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57417)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57416](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57416)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57419](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57419)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57420](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57420)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57435](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57435)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57429](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57429)

#### 4、Microsoft 产品安全漏洞

Microsoft Windows Phone 7 是微软推出的一款智能手机操作系统；Microsoft Internet Explorer 是微软公司推出的一款网页浏览器。本周，上述两款微软产品被披露存在多个漏洞，攻击者利用漏洞可在手机和邮件服务器通信过程中发起中间人攻击；诱使用户访问恶意网页执行挂马攻击，从而控制用户系统。

CNVD 收录的相关漏洞包括：Microsoft Windows Phone 7 SSL 证书'Common Name'校验安全绕过漏洞、Microsoft IE execCommand 内存错误引用漏洞。目前，厂商已经发布补丁信息修复 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=57449](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57449)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=57343](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57343)

#### 5、VBulletin 'blog\_plugin\_useradmin.php' SQL 注入漏洞

VBulletin 是一款基于 PHP 的论坛建站软件。本周，VBulletin 被披露存在一个综合评级为“高危”的 SQL 注入漏洞。由于 VBulletin 'blog\_plugin\_useradmin.php'脚本未能正确过滤用户提交的输入，攻击者利用漏洞可发起 SQL 注入攻击，获得数据库信息。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/sites/main/preview/ldgg\\_preview.htm?tid=57735](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=57735)

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                                   | 综合评级 | 修复方式                                                                                                                                                                                                      |
|-----------------|----------------------------------------|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CNVD-2012-14676 | Google SketchUp '.SKP'文件内存破坏漏洞         | 高    | Google 已经修复此漏洞，建议用户下载使用：<br><a href="http://support.google.com/sketchup/bin/static.py?hl=en">http://support.google.com/sketchup/bin/static.py?hl=en</a>                                                   |
| CNVD-2012-14658 | SumatraPDF 内存破坏漏洞<br>(CNVD-2012-14658) | 高    | SumatraPDF Reader software 2.1 已经修复此漏洞，建议用户下载使用：<br><a href="http://blog.kowalczyk.info/software/sumatrapdf/free-pdf-reader.html">http://blog.kowalczyk.info/software/sumatrapdf/free-pdf-reader.html</a> |

|                 |                                                        |   |                                                                                                                                                                                                                                                                                       |
|-----------------|--------------------------------------------------------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CNVD-2012-14662 | Novo Knowledge Base Enterprise Edition SQL 注入漏洞        | 高 | 暂无                                                                                                                                                                                                                                                                                    |
| CNVD-2012-14656 | SumatraPDF 内存破坏漏洞 (CNVD-2012-14656)                    | 高 | 厂商已经修复此漏洞，建议用户下载使用：<br><a href="http://blog.kowalczyk.info/software/sumatrapdf/free-pdf-reader.html">http://blog.kowalczyk.info/software/sumatrapdf/free-pdf-reader.html</a>                                                                                                          |
| CNVD-2012-14639 | TAGWORX.CMS 'cid'参数 SQL 注入漏洞                           | 高 | 暂无                                                                                                                                                                                                                                                                                    |
| CNVD-2012-14626 | Jenkins Continuous Integration Game 插件跨站脚本漏洞           | 高 | 厂商已经修复此漏洞，建议用户下载使用：<br><a href="https://wiki.jenkins-ci.org/display/JENKINS/The+Continuous+Integration+Game+plugin">https://wiki.jenkins-ci.org/display/JENKINS/The Continuous Integration Game plugin</a>                                                                            |
| CNVD-2012-14583 | Debian devscripts 任意代码执行漏洞 (CNVD-2012-14583)           | 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.debian.org/security/2012/dsa-2549">http://www.debian.org/security/2012/dsa-2549</a>                                                                                                                                                   |
| CNVD-2012-14636 | osCommerce PayPal 网站支付标准模块安全绕过漏洞                       | 高 | 厂商已经修复此漏洞，建议用户下载使用：<br><a href="https://github.com/osCommerce/oscommerce2/tree/master/catalog/ext/modules/payment/paypal">https://github.com/osCommerce/oscommerce2/tree/master/catalog/ext/modules/payment/paypal</a><br><a href="http://oscommerce.com/">http://oscommerce.com/</a> |
| CNVD-2012-14599 | NCMedia Sound Editor Pro 'MRUList201202.dat'文件栈缓冲区溢出漏洞 | 高 | 暂无                                                                                                                                                                                                                                                                                    |
| CNVD-2012-14620 | HP Operations Orchestration 远程代码执行漏洞                   | 高 | HP 已修复此漏洞，建议用户下载使用：<br><a href="http://support.openview.hp.com/downloads.jsp">http://support.openview.hp.com/downloads.jsp</a>                                                                                                                                                        |
| CNVD-2012-14605 | OptiPNG 内存错误引用远程代码执行漏洞                                 | 高 | OptiPNG 0.7.3 已经修复此漏洞，建议用户下载使用：<br><a href="http://sourceforge.net/news/?group_id=151404">http://sourceforge.net/news/?group_id=151404</a>                                                                                                                                            |

表 3 部分高危漏洞列表

小结：本周，Cisco 多个产品被披露存在多个安全漏洞，攻击者利用漏洞可获得数据库信息或劫持用户会话、发起拒绝服务攻击，企业用户和网络管理员需重点进行防范；而 Microsoft IE 浏览器以及 Apple 多款产品被披露存在零日漏洞，攻击者利用漏洞发起基于社会工程学的攻击和远程挂马攻击，导致终端用户面临较为严重的威胁。此外，VBulletin 和 Drupal 等网站内容管理软件也被披露存在高危漏洞或零日漏洞，由于应用广泛，网站管理员需加强防范。

## 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、McAfee 布升级程序，修补 McAfee Application Control 漏洞

McAfee Application Control 通过使用动态的信任模型，保护企业的服务器和终端免受未经授权应用程序和恶意软件的威胁。本周，McAfee 发布升级程序，修补了 McAfee Application Control 存在的漏洞。攻击者可以利用漏洞绕过文件自动运行控制，构建特制的文件在系统上执行。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=22456](http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=22456)

## 本周要闻速递

### 1. 微软发布工具修复 IE 浏览器中安全漏洞

9 月 21 日消息：微软在昨天放出了紧急修复工具 Fix it，用来修复 IE 浏览器中存在的 0day 安全漏洞。据悉，Fix it 修复工具的使用方法非常简单，用户只需要一键点击就可以完成修复。此外，微软还将通过 Windows Update 发布一个安全补丁，该补丁将彻底修复 IE 中存在的安全问题。0day 在上周被一名国外的安全专家发现，该漏洞可以被黑客利用绕过 Windows 的 ASLR 防护机制，访问任何计算机用户曾访问过的文件。受此影响的包括 Windows XP、Vista 和 Windows 7 中的 IE 浏览器，IE7、IE8 和 IE9 均未能幸免。

参考链接：<http://www.lntv.com.cn/ltnv/newindex/kjdt/201209/24-268566.html>

### 2. 甲骨文“漏洞百出”

据国外媒体报道，近日“漏洞百出”的甲骨文再次被曝其存有身份验证协议漏洞。黑客可利用身份漏洞轻松地破解甲骨文的数据库。该漏洞能让任何人以非法手段攻击和访问数据。在今天阿根廷安全会议上，研究人员的调查结果显示，确实存在身份验证攻击的事实。

参考链接：<http://www.lupaworld.com/article-220138-1.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