

## 信息安全漏洞周报

2010 年 12 月 13 日-2010 年 12 月 19 日

2010 年第 49 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 114 个，其中高危漏洞 35 个、中危漏洞 21 个、低危漏洞 58 个。上述漏洞中，可利用来实施远程攻击的漏洞有 91 个。经跟踪发现，网上已经出现针对“PHP GD 扩展'imagemagick()'函数栈缓冲区溢出漏洞”、“Linksys WRT54G2/BEFSR41 跨站请求伪造漏洞”和“CA Internet Security Suite KmxSbx.sys 整数溢出漏洞”等的零日攻击代码，请使用相关产品的用户注意做好防护措施。本周收录的安全漏洞中，已有 92 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、Microsoft 多个产品存在安全漏洞

本周，Microsoft 发布了 12 月安全公告，公布并修复了 Windows 操作系统、IE 浏览器、Office 等软件存在的多个安全漏洞。其中“高危”漏洞共 23 个，具体漏洞包括：Microsoft Windows Address Book "wab32res.dll" DLL 加载任意代码执行漏洞(MS10-096)、Microsoft Windows OpenType Font (OTF)驱动两次释放远程代码执行漏洞、Microsoft Windows OpenType Font (OTF)驱动非法数组远程代码执行漏洞、Microsoft Windows OpenType Font (OTF)驱动 CMAP 表远程代码执行漏洞、Microsoft Publisher 数组索引内存破坏远程代码执行漏洞、Microsoft Publisher 大小值堆内存破坏远程代码执行漏洞、Microsoft Publisher 'pubconv.dll'堆缓冲区溢出远程代码执行漏洞、Microsoft Publisher 'pubconv.dll'数组索引内存破坏远程代码执行漏洞、Microsoft Publisher (CVE-2010-3954)内存破坏远程代码执行漏洞、Microsoft Office TIFF 图像转换器(CVE-2010-3950)内存破坏漏洞、Microsoft Office CGM 图像转换器缓冲区溢出漏洞(CVE-2010-3945)、Microsoft Windows BranchCache DLL 装载任意代码执行漏洞(CVE-2010-3966)、Microsoft Office PICT 图像转换器(CVE-2010-3946)整数溢出漏洞、Microsoft Office TIFF 图像转换器(CVE-2010-3947)基于堆的缓冲区溢出漏

洞、Microsoft Office TIFF 图像转换器(CVE-2010-3949)内存破坏漏洞、Microsoft Office FlashPix 图像转换器 (CVE-2010-3951)堆缓冲区溢出漏洞、Microsoft Office FlashPix 图像转换器 (CVE-2010-3952)堆缓冲区溢出漏洞、Microsoft Internet Explorer 未初始化对象内存破坏漏洞 (CVE-2010-3340)、Microsoft Internet Explorer 跨域信息漏洞 (CVE-2010-3342)、Microsoft Internet Explorer 跨域信息漏洞 (CVE-2010-3348)、Microsoft Internet Explorer 未初始化对象内存破坏漏洞 (CVE-2010-3343)、Microsoft Internet Explorer 选择 HTML 元素释放后使用内存破坏漏洞、Microsoft Internet Explorer 未初始化 HTML 元素远程代码执行漏洞 (CVE-2010-3346) 等。攻击者可以利用这些漏洞发起执行任意代码攻击或获取用户权限。目前，Microsoft 已经发布了补丁程序修复这些漏洞，CNVD 建议用户及时下载更新，避免引发此类漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03375>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03346>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03343>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03341>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03338>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03337>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03336>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03335>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03334>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03333>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03332>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03331>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03330>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03329>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03327>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03326>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03324>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03317>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03316>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03315>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03314>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03312>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03311>

## 2. Google Chrome 存在多个安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。本周，Google Chrome 出现 3 个安全等级为“高”的漏洞，攻击者可以利用这些漏洞破坏内存或导致用户应用程序崩溃。CNVD 本周收录的 Google Chrome 漏洞包括：Google Chrome 光标处理存在未明漏洞、Google Chrome

在解析 CSS 时存在漏洞、Google Chrome 执行消息反序列化时存在验证漏洞。目前，Google 已经发布了补丁程序修复这些漏洞，CNVD 建议用户及时下载更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03355>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03354>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03352>

### 3、Novell 产品存在多个安全漏洞

本周，Novell 的 ZENworks Handheld Management、Vibe 和 iPrint Client 产品出现了多个安全漏洞。ZENworks Desktop Management 是 Novell 提供的桌面管理解决方案，iPrint 是打印解决方案，而 Vibe 则是一个社交媒体平台。CNVD 本周收录的漏洞包括：Novell ZENworks Desktop Management 'ZenRem32.exe'缓冲区溢出漏洞、Novell ZENworks Desktop Management 'tftpd'组件缓冲区溢出漏洞、Novell iPrint Client 多个远程代码执行漏洞、Novell Vibe 3 BETA OnPrem 'select\_single'字段类型 HTML 注入漏洞。攻击者可以利用这些漏洞实施执行任意代码和拒绝服务攻击。除“Novell iPrint Client 多个远程代码执行漏洞”外，厂商已经发布了其余漏洞的补丁，CNVD 建议广大 Novell 用户及时下载更新，避免引发此类漏洞的相关安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03284>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03283>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03259>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03251>

### 4、IBM Tivoli Storage Manager Client 存在多个安全漏洞

Tivoli Storage Manager (TSM) Client 是 IBM 提供的一款企业级数据备份和恢复软件。本周，IBM Tivoli Storage Manager Client 出现了多个安全漏洞，攻击者可以利用这些漏洞获得敏感信息或劫持目标用户会话。CNVD 本周收录的相关漏洞包括：IBM Tivoli Storage Manager Client 存在分级存储管理客户端安全漏洞、IBM Tivoli Storage Manager Client 存在未明错误安全漏洞、IBM Tivoli Storage Manager Client 存在缓冲区溢出安全漏洞。目前，厂商已经发布了补丁程序修复这些漏洞，CNVD 建议用户及时下载使用，避免引发此漏洞的相关安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03370>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03368>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03367>

### 5、Apple 存在多个安全漏洞

本周，Apple 的 Time Capsule 和 AirPort Base Station 出现多个安全漏洞。Time Capsule 是一款可让 Mac 和 PC 通过无线网络进行数据备份的应用软件，AirPort Base Station 是一款无线基站服务软件。CNVD 本周收录的 Apple 漏洞包括：Apple Time Capsule/AirPort Base Station 网桥实现存在错误安全漏洞、Apple Time Capsule/AirPort Base Station 存在绕过一些

基于 IP 限制的服务安全漏洞、Apple Time Capsule/AirPort Base Station 存在资源耗竭错误漏洞。远程攻击者可以利用漏洞进行拒绝服务攻击或绕过 IP 限制进行访问。目前，Apple 已经发布了漏洞的补丁程序，CNVD 建议用户及时下载使用，避免引发此漏洞的相关安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03377>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03376>  
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03373>

**小结：**本周，Microsoft 发布了 12 月安全公告，修复了 Windows 操作系统、IE 浏览器、MS Office 等软件存在的多个安全漏洞。攻击者可以利用这些漏洞实施远程任意代码执行、权限提升、拒绝服务等攻击。CNVD 已经收录了漏洞的补丁程序，提醒广大微软用户及时下载更新。另外，Google Chrome、IBM Tivoli Storage Manager、Apple Time Capsule/AirPort Base Station、Novell ZENworks Handheld Management/Vibe/ iPrint Client 等产品均出现了安全漏洞，对国内用户的信息安全和互联网网络安全构成较为威胁，请使用上述软件的相关机构和个人及时采取安全防范措施。

## 本周重要漏洞修补信息

本周，CNVD 整理和发布以下重要安全修补信息。

### 1、Opera Web 浏览器发布升级程序修补了多个安全漏洞

Opera Web Browser 是一款开源的 WEB 浏览器。本周，Opera Web Browser 发布了多个升级程序用于修复多个安全漏洞，以避免攻击者利用漏洞获得敏感信息或获得数据管理权限。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/patch/2152>  
<http://www.cnvd.org.cn/patch/2153>  
<http://www.cnvd.org.cn/patch/2154>

## 本周要闻速递

### 1.微软发布 2010 年最后一次安全更新，批量修复 40 个漏洞

12 月 15 日，微软发布了 2010 年最后一次例行的安全更新，共发布了 17 个安全补丁，用于修复 Windows 操作系统、IE 浏览器、Office 软件相关的 40 个漏洞，其中包括被“Stuxnet”（有媒体称“超级工厂病毒”）利用的一个漏洞以及 11 月初曝光的 IE 浏览器 CSS 0day 漏洞。此次微软发布的 17 个补丁中，2 个的安全级别定为“严重”，14 个定为“重要”，1 个定为“中等”。安全专家表示，微软如此罕见的大规模批量修复漏洞，是迫于日益紧张

的安全环境。但由于补丁具有“滞后性”的特点，网民还需要使用专业的杀毒软件为电脑提供全面防护。

参考链接：<http://www.cnetnews.com.cn/2010/1215/1966365.shtml>

## 2. 维基解密拥护者向相关网站发动拒绝服务攻击以示不满

近日，维基解密拥护者向万事达、Visa、瑞典政府网、瑞士 PostFinance 银行以及其他网站发动了拒绝式服务攻击。尽管近年来攻击者的动机多是在于资金获取，这次“hacktivism”可被视为出于“特别目的”。维基解密受到强大的压力，已经停止继续发布美国机密外交文传电报。迫于美国政府压力，相关企业已停止与维基解密有关运作或捐款。对此，“匿名行动”的黑客成员共同利用攻击工具，快速发动了一次分布式拒绝服务攻击（DDoS）以抵制任何企图反对维基解密的公司。

参考链接：[http://tech.ccidnet.com/art/1099/20101216/2272249\\_1.html](http://tech.ccidnet.com/art/1099/20101216/2272249_1.html)

## 3. 网站账户信息泄露，曝光最流行密码

上周末，旗下拥有 Gizmodo、Kotaku、Lifehack 等多个知名博客的 Gawker Media 服务器被黑客攻破，超过 100 万份用户资料在网络上曝光。这些资料包含用户名、邮箱地址以及密码。虽然密码大部分为加密存储，但不久后，其中 188279 个账户的密码也被解密泄露出来。华尔街日报根据这些信息做了一项有趣的统计，即在这 188279 个密码中，查找最常见的密码选择。不出所料，排名第一的密码就是“123456”，有超过 3000 人使用。排名它之后的是 password、12345678、qwerty、abc123、111111 等。Gawker 旗下网站的名字如 lifehack、consumer、gizmodo、gawker、kotaku 也都是常见密码。

参考链接：<http://www.hackbase.com/news/2010-12-16/40071.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