

信息安全漏洞周报

2010 年 11 月 29 日-2010 年 12 月 05 日

2010 年第 47 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低。

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 88 个，其中高危漏洞 10 个、中危漏洞 36 个、低危漏洞 42 个。上述漏洞中，可利用来实施远程攻击的漏洞有 64 个。经跟踪发现，网上已经出现针对“Microsoft Internet Explorer 中执行无效的标记代码的漏洞”、“Free Simple Software download 模块 SQL 注入漏洞”、“Yaws URI 目录遍历漏洞”以及“Elxis CMS SQL 注入漏洞”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 60 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、Linux Kernel 出现多个安全漏洞

Linux Kernel 是开源操作系统 Linux 所使用的内核。本周，Linux Kernel 出现了多个安全漏洞，攻击者可以利用漏洞发起提升特权、获取敏感信息或拒绝服务等攻击。CNVD 本周收录的相关漏洞包括：Linux Kernel net/sctp/auth.c 文件资源管理错误漏洞、Linux Kernel KVM 实现资源管理错误漏洞、Linux Kernel Video4Linux 输入验证漏洞、Linux Kernel DRM 子系统输入验证漏洞、Linux Kernel 本地地址限制控制安全漏洞、Linux Kernel uart_get_count 函数信息泄露漏洞、Linux Kernel rs_ioctl 函数信息泄露漏洞、Linux Kernel sisfb_ioctl 函数信息泄露漏洞、Linux Kernel 拒绝服务漏洞、Linux Kernel 'pipe_fcntl()'本地拒绝服务漏洞、Linux Kernel 'x25_parse_facilities()' CVE-2010-4164 远程拒绝服务漏洞、Linux Kernel TIOCGICOUNT CVE-2010-4073 信息泄漏漏洞、Linux Kernel TIOCGICOUNT CVE-2010-4074 信息泄漏漏洞、Linux Kernel "setup_arg_pages()"本地拒绝服务漏洞。其中“Linux Kernel DRM 子系统输入验证漏洞”和“Linux Kernel net/sctp/auth.c 文件资源管理错误漏洞”的安全等级为“高”。除“Linux Kernel 'posix-cpu-timers.c'本地竞争条件漏

洞”外，Linux 已经发布升级补丁修复其余漏洞，CNVD 建议用户关注厂商主页以获得修补方案。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03125>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03122>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03118>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03103>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03094>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03093>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03092>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03091>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03090>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03062>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03053>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03052>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03051>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03050>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03044>

2. Microsoft 多个产品存在安全漏洞

本周，Microsoft 的 Internet Explorer 浏览器、Windows 操作系统和 Outlook 软件等产品出现多个安全漏洞。CNVD 收录的漏洞包括：Microsoft Internet Explorer 中执行无效的标记代码的漏洞、Microsoft Windows win32k.sys 驱动"GreEnableEUDC()"权限提升漏洞、Microsoft Outlook 邮件附件处理拒绝服务漏洞。其中“Microsoft Outlook 邮件附件处理拒绝服务漏洞”的安全等级为“高”。攻击者利用这些漏洞可以进行拒绝服务和执行任意代码攻击。目前，Microsoft 还未发布升级补丁修复这些安全漏洞，CNVD 建议广大 Microsoft 用户关注厂商的主页以获取最新版本，避免引发此漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03078>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03046>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03045>

3. Apple 多款产品存在多个安全漏洞

本周，Apple 的 WebKit、Safari 产品出现了多个安全漏洞。WebKit 是开源的 WEB 浏览器引擎，目前被 Safari、Chrome 等浏览器使用。Safari 是苹果家族操作系统默认所捆绑的 WEB 浏览器。CNVD 收录的具体漏洞包括：Apple iOS WebKit 权限许可和访问控制漏洞、Apple iPhone 和 iPod touch Safari 用户界面可欺骗漏洞。攻击者可以利用漏洞获取敏感信息或执行网上钓鱼类型的攻击。其中，“Apple iOS WebKit 权限许可和访问控制漏洞”的安全等级为“高”。目前，Apple 已经发布了这个高危漏洞的补丁，用户可随时下载使用。而对于“Apple iPhone 和 iPod touch Safari 用户界面可欺骗漏洞”，Apple 还未发布相关的补

丁，CNVD 提醒使用此软件的用户随时关注厂商的主页以获取最新版本，避免引发此漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03123>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03112>

4、ProFTPD 存在安全漏洞

ProFTPD 是一款 FTP 服务端软件。本周 CNVD 收录的 ProFTPD 漏洞包括：ProFTPD 源入侵后门未授权访问漏洞、ProFTPD 'mod_sql'远程堆缓冲区溢出漏洞。其中，“ProFTPD 源入侵后门未授权访问漏洞”的安全等级为“高”。攻击者可以利用这些漏洞获取 root 权限。目前厂商已经发布了“ProFTPD 源入侵后门未授权访问漏洞”的补丁程序，但尚未发布“ProFTPD 'mod_sql'远程堆缓冲区溢出漏洞”的补丁，CNVD 提醒使用此软件的用户及时下载补丁更新或关注厂商的主页以获取最新版本，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-2010-03107>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03106>

5、Winamp 存在多个安全漏洞

Winamp 是一款流行的媒体播放软件。本周 CNVD 收录的 Winamp 漏洞包括：Winamp "in_midi"中存在整数溢出漏洞、Winamp "in_nsv.dll"插件存在整数溢出漏洞。攻击者可以利用漏洞进行拒绝服务或执行任意代码攻击。这两个漏洞的安全等级都为“高”。目前厂商已经发布漏洞的补丁，CNVD 建议用户下载使用，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-2010-03075>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03074>

小结：本周，Linux、Apple、Microsoft 等厂商的产品出现了多个安全漏洞，对国内用户的信息安全和互联网网络安全构成较为严重的威胁，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、MIT Kerberos 发布升级程序修补了多个安全漏洞

Kerberos 是一款使用强壮的加密来验证客户端和服务端端的网络协议。本周，CNVD 收录了 MIT Kerberos 的多个安全漏洞，攻击者可以利用这些漏洞绕过限制执行未授权操作。目前，厂商已经发布了漏洞的升级修补程序，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/1899>
<http://www.cnvd.org.cn/patch/1900>

<http://www.cnvd.org.cn/patch/1902>
<http://www.cnvd.org.cn/patch/1903>

本周要闻速递

1.Chrome 8.0 正式版发布：修复超过 800 个 Bug

Chrome 推出了首个 Chrome 8.0 正式版本，本次更新除了超过 800 个 Bug 修复以及大量的稳定性改进之外，还集成了受沙箱保护的 PDF 查看工具。本次一共修复了 13 个重要的安全漏洞，其中包括 4 个低风险漏洞、5 个中风险漏洞和 4 个高风险漏洞。另外，Chrome Beta 分支也同时更新到了该版本。

参考链接：<http://www.donews.com/net/201012/293568.shtml>

2. AVG 最新升级可导致 64 位 Windows 7 崩溃

12 月 1 日，AVG 推送的更新可以造成 64 位 PC 上运行的 Windows 7 彻底崩溃。问题出在 271.1.1/3292 (432/3292)数据库更新阶段，当更新完毕，软件会提示重新启动，这时受影响的电脑就会弹出一个 C0000135 错误，无法启动。目前，AVG 已经紧急更新以保证更多的计算机不受影响，并公布了如何禁用软件的解决方案，AVG 的论坛用户也想出了一些解决问题的技巧，例如按 F8 键进入安全模式删除 AVG 更新。

参考链接：<http://www.cnbeta.com/articles/128729.htm>

3. Windows Phone 7 安全性受质疑

最近，微软公司全新 Windows Phone 7 应用下载服务器上被披露存在一个漏洞。注册开发人员可以使用“未加锁”的电话，直接从微软的在线服务器上下载微软 XAP 文件格式的基本代码包，而且可以完全绕过该公司的 Zune 市场，而后，使用多种人们熟知的工具就可以将 XAP“包”中的文件分解为各个组成部分，包括保密数据或知识产权。之所以这么容易解包，主要原因在于 Windows Phone 7 应用的下层基础——微软.Net 代码框架的某个版本。该应用代码可在虚拟机中运行，由虚拟机将其翻译并调用下层操作系统。对于 WP7 而言，采用 Microsoft Silverlight 或 Microsoft XNA Studio 都可以提供虚拟机。微软很快就关闭了这个特定的 XAP 文件下载漏洞，所幸的是这种情况只适用于注册程序员的手机，普通消费者的 WP7 手机并不适用。

参考链接：http://security.zdnet.com.cn/security_zone/2010/1202/1955938.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

邮箱：vreport@cert.org.cn

电话：010-82990999