

信息安全漏洞周报

2011 年 3 月 7 日-2011 年 3 月 13 日

2011 年第 10 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 134 个，其中高危漏洞 42 个、中危漏洞 18 个、低危漏洞 74 个。上述漏洞中，可利用来实施远程攻击的漏洞有 125 个。网上已经出现针对“.NET Runtime Optimization Service 本地提权漏洞”和“Apple QuickTime '.m3u'文件远程栈缓冲区溢出漏洞”等零日漏洞的攻击代码，请使用相关产品的用户注意做好防护措施。本周收录的漏洞中，已有 94 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、亚控公司 Kingview 缓冲区溢出漏洞

2010 年 3 月 8 日，CNVD 获知北京亚控科技发展有限公司（简称亚控公司）推出的一款工业控制软件 Kingview 存在安全漏洞，受漏洞影响的软件版本包括 Kingview6.5.2 和 6.5.3。CNVD 第一时间对漏洞的真实性进行了验证，并将相关情况通报亚控公司。3 月 9 日，亚控公司完成了对漏洞的技术分析，并于 3 月 10 日发布了官方补丁程序。根据亚控公司提供的信息，Kingview 主要应用于工业自动化的过程控制和管理监控领域，用户主要分布在国内外机械、机电、电力、水处理等行业。为有效应对漏洞带来的安全威胁，CNVD 建议 Kingview 6.5.2 和 6.5.3 的用户及时采取如下防范措施：（1）及时下载亚控公司官方发布的漏洞补丁程序，对系统进行安全加固。（2）将漏洞影响主机与互联网进行物理隔离，以免使攻击者有可乘之机。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04541>

2、Microsoft 产品安全漏洞

本周，微软发布了 2011 年 3 月份的月度例行安全公告，共包含三项安全更新，其中一项更新的综合评级为“严重”，其余两项为“重要”。本次发布的安全更新修复了 Microsoft Windows 和 Office 中存在的多个安全漏洞，攻击者可以利用这些漏洞实施远程攻击，攻击一旦成功就可在受害主机上执行任意代码，获得系统管理操作权限。CNVD 收录的漏洞包

括：Microsoft Windows Media Player/Windows Media Center '.dvr-ms'文件代码执行漏洞、Microsoft 远程桌面连接客户端 DLL 装载任意代码执行漏洞、Microsoft DirectShow DLL 装载任意代码执行漏洞。CNVD 提醒广大微软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/vulnerability/CNVD-2011-04581>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04579>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04569>

3、Apple 产品安全漏洞

本周，Apple 公司在其官方网站发布安全公告及安全更新，修复了 iTunes 软件中存在的 57 个安全漏洞。其中，有 50 个漏洞是由于开源浏览器引擎 WebKit 存在内存破坏缺陷引起的。攻击者可以利用该漏洞发起中间人攻击，严重的可致应用程序意外终止或转而执行攻击者构造的任意指令。CNVD 收录的漏洞包括：Apple WebKit 任意代码执行漏洞（CVE-2011-0125、CVE-2011-0126、CVE-2011-0127、CVE-2011-0128、CVE-2011-0129、CVE-2011-0130）、Apple iPhone Webkit 库 Javascript 数组 sort 方法远程代码执行漏洞、Apple iTunes JPEG 图形堆缓冲区溢出漏洞等。上述漏洞的综合评级均为“高危”，CNVD 提醒广大用户及时下载更新，避免引发漏洞相关的安全事件。此外，Apple 的产品 QuickTime 被披露存在一个远程栈缓冲区溢出漏洞，互联网上已经出现了针对该漏洞的攻击代码，主要影响 QuickTime Player 7.5 和 7.5.5 版本。目前，Apple 尚未发布该漏洞的补丁程序，CNVD 提醒广大用户随时关注厂商主页以获取补丁程序或最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04590>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04529>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04528>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04527>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04526>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04525>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04524>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04503>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04497>

4、Google Chrome 安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，GoogleChrome 被披露存在多个安全漏洞。攻击者可以利用漏洞发起拒绝服务攻击、获取敏感信息或执行任意代码。CNVD 收录的具体漏洞包括：Google Chrome 内存破坏漏洞、Google Chrome 非法内存访问漏洞、Google ChromeDOM 树破坏漏洞、Google Chrome 光标处理漏洞、Google Chrome 堆地址泄露漏洞、Google Chrome 失效指针漏洞、Google Chrome 文本渲染赋值漏洞、Google Chrome 浏览器漏洞、Google Chrome 视频编码漏洞、Google Chrome 失效指针漏洞。目前，Google 已经发布了补丁程序修复这些漏洞，CNVD 提醒广大用户及时下载更新，避免引发

漏洞相关的安全事件。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-04580>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04578>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04577>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04576>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04574>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04573>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04572>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04570>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04568>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-04567>

5、.NET Runtime Optimization Service 本地提权漏洞

.NET Runtime Optimization Service 是.NET 运行优化服务进程。.NET Runtime Optimization Service 的 mscorsvw.exe（在默认权限设置时）能被任何非管理员的域用户以及本地的 power users 用户组重写或覆盖，从而导致权限提升。该漏洞的综合评级为“高危”。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响.NET Runtime Optimization Service 2.0.50727 版本，而厂商尚未发布该漏洞补丁程序。CNVD 建议用户及时关注厂商主页，以获取补丁程序或最新版本。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-04546>

小结：上述漏洞中，北京亚控科技有限公司 KingView6.5.2/6.5.3 软件产品存在的漏洞是国外漏洞研究者发现的关于这款产品的第二个高危漏洞。该漏洞对相关的机械、机电、电力、水处理等行业企业的生产系统运行安全构成较为严重的威胁。此外，本周微软发布了 2011 年 3 月份的月度例行安全公告，修复了 Microsoft Windows 和 Office 中存在的多个安全漏洞；Apple 发布安全公告，修复 iTunes 软件中存在的多个安全漏洞；Google Chrome 浏览器、.NET Runtime Optimization Service 运行优化服务进程均出现了安全漏洞。上述漏洞若未能及时修补，会对互联网网络安全及用户个人信息安全构成威胁，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、Linux 发布升级程序，修补 Kernel 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 发布升级程序，修补了 Kernel 多个安全漏洞，避免攻击者利用漏洞发起拒绝服务攻击或提升特权。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/3258>
<http://www.cnvd.org.cn/patch/3227>
<http://www.cnvd.org.cn/patch/3210>
<http://www.cnvd.org.cn/patch/3216>



本周要闻速递

1.Android 曝后门木马利用系统溢出漏洞获取 ROOT 权限

近日, 国内知名安全厂商拦截到一批新型 Android 木马——“安卓卧底”, 该类木马在窃取用户隐私的同时, 可以利用系统溢出漏洞获取 ROOT 权限(系统最高的管理员权限), 使黑客可以通过云端指令控制用户手机, 实现包括删除系统文件、程序, 甚至窃取几乎所有文件的操作。可以说, 用户手机一旦感染, 就完全沦为“肉鸡”。安全专家表示, “安卓卧底”系列木马为隐私窃取类木马, 从代码级别直接篡改正常软件, 隐蔽性极高, 非专业工具基本上无法识别。所以, 用户应选择知名软件商店及网站或下载绝对安全的 Android 应用; 如果发现话费莫名减少, 流量无故消失等情况, 应立即使用专杀工具进行木马查杀。参考链接: <http://tech.sina.com.cn/s/2011-03-08/14215260134.shtml>

2. 苹果发布安全补丁修复 Safari 漏洞

3月11日消息, 据国外媒体报道, 苹果已经发布了62个Safari浏览器漏洞修复程序, 并警告用户, 如果不打补丁, 所有的漏洞可能导致很多问题。这一系列的更新与WebKit有很大的关系, Mac OS X v10.5.8、Mac OS X Server v10.5.8、Mac OS X v10.6.5或更高版本, Mac OS X Server v10.6.5或更高版本, Windows 7、Vista、XP SP2或更高版本都配备了该功能。安全专家敦促广大用户尽快下载安装相关的更新补丁。参考链接: http://tech.ccidnet.com/art/1099/20110311/2330985_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

邮箱：vreport@cert.org.cn

电话：010-82990999