

信息安全漏洞周报

2010 年 12 月 27 日-2011 年 1 月 2 日

2010 年第 51 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 52 个，其中高危漏洞 4 个、中危漏洞 15 个、低危漏洞 33 个。上述漏洞中，可利用来实施远程攻击的漏洞有 45 个。经跟踪发现，网上已经出现针对“Microsoft Windows Fax 封面编辑器远程代码执行漏洞”、“Apple QuickTime Pictureviewer '.jp2' 文件拒绝服务漏洞”、“Chilkat FTP2 ActiveX 控件多个不安全方法漏洞”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 27 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、IBM 多款产品存在安全漏洞

本周，IBM 的产品 Tivoli Storage Manager、Lotus Mobile Connect、Tivoli Access Manager 出现了多个安全漏洞。IBM Tivoli Storage Manager 是一款数据存储与备份管理解决方案；Lotus Mobile Connect 是一个分布式、多用途的通信平台；Tivoli Access Manager 是一款基于策略的电子商务访问控制解决方案。CNVD 本周收录的 IBM 漏洞包括：IBM Tivoli Access Manager for e-business 目录遍历漏洞、IBM Lotus Mobile Connect LTPA 令牌客户端访问漏洞、IBM Lotus Mobile Connect HTTP-TCP 会话拒绝服务漏洞、IBM Lotus Mobile Connect Manager 参考计数器漏洞、IBM Tivoli Storage Manager backup-archive 客户端任意文件重写漏洞、IBM Tivoli Storage Manager 远程代码执行漏洞。攻击者可以利用这些漏洞执行任意代码导致用户敏感信息泄露或进行拒绝服务攻击。其中“IBM Tivoli Access Manager for e-business 目录遍历漏洞”的安全等级为“高”，目前 IBM 尚未发布此漏洞的补丁程序。而对本周收集的其余 IBM 漏洞，IBM 已经发布了修复补丁，CNVD 建议广大用户及时下载更新，避免引发漏洞的相关安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03550>

<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03549>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03532>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03531>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03530>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03517>

2、Microsoft Windows Fax 封面编辑器远程代码执行漏洞

Microsoft Windows 是一款流行的操作系统。Microsoft Windows 包含的传真封面页编辑器(fxscover.exe)在处理.cov 文件时"CDrawPoly::Serialize()"函数存在缓冲区溢出漏洞，攻击者通过构建包含超大记录的.cov 文件，诱使用户打开解析，可使得攻击者在用户主机上执行事先构造的恶意代码，进而控制用户主机。该漏洞目前级别为“高危”，经 CNVD 跟踪发现，互联网上已经出现针对这个漏洞的恶意代码攻击。目前 Microsoft 尚未发布该漏洞的补丁程序，CNVD 建议广大用户及时关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03520>

3、Linux Kernel 存在多个安全漏洞

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，CNVD 收录的漏洞包括：Linux Kernel Controller Area Network 信息泄露漏洞、Linux Kernel drivers/scsi/bfa/bfa_core.c 文件拒绝服务漏洞、Linux Kernel viafb_ioctl_get_via_fb_info 函数信息泄露漏洞。攻击者可以利用这些漏洞获取敏感信息。目前 Linux 已经发布了补丁程序修复这些漏洞，CNVD 建议广大用户及时下载更新，避免引发漏洞的相关安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03564>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03548>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03528>

4、Joomla! 出现多个安全漏洞

Joomla! 是一款开源内容管理系统。本周，CNVD 收录的 Joomla! 漏洞包括：Joomla! JotLoader 组件目录遍历漏洞、Joomla! Algis Info aiContactSafe 组件跨站脚本攻击漏洞。攻击者可以利用这些漏洞获取敏感信息或修改未授权信息。其中“Joomla! JotLoader 组件目录遍历漏洞”的安全等级为“高”，目前厂商尚未发布此漏洞的补丁程序。对于“Joomla! Algis Info aiContactSafe 组件跨站脚本攻击漏洞”，厂商已经发布了漏洞的补丁程序，CNVD 建议用户及时采取相关措施，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-2010-03562>
<http://www.cnvd.org.cn/vulnerability/ CNVD-2010-03547>

5、Chilkat FTP2 ActiveX 控件多个不安全方法漏洞

Chilkat FTP2 是一款商业文件传输协议组件（又称 FTP 服务器软件）。利用 Chilkat FTP2 ActiveX 组件(ChilkatFtp2.DLL 2.6.1.1)调用不安全的"GetFile()"或"PutFile()"等方法，攻击者可以通过构建恶意网面，诱使用户访问，进而获取和覆盖文件服务器上的任意文件。

此漏洞的安全等级为“高”。厂商目前尚未发布此漏洞补丁程序，CNVD 建议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/vulnerability/CNVD-2010-03538>

小结：本周，Microsoft Windows 出现了一个打印封面编辑器远程代码执行漏洞，攻击者可以利用这个漏洞以应用程序安全上下文执行任意代码。经 CNVD 跟踪发现，互联网上已经出现针对这个漏洞的恶意代码攻击，对广大微软用户造成了较为严重的威胁。此外，IBM 的产品 Tivoli Storage Manager、Lotus Mobile Connect、Tivoli Access Manager，Linux Kernel 和 Joomla! 内容管理系统均出现了多个安全漏洞。这些产品在国内用户中使用已经越来越广泛，这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、Novell iPrint Client 发布升级程序修补了多个安全漏洞

Novell iPrint Client 打印解决方案允许用户向网络打印机发送文档。本周，Novell iPrint Client 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执行任意指令。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/2446>
<http://www.cnvd.org.cn/patch/2447>
<http://www.cnvd.org.cn/patch/2448>
<http://www.cnvd.org.cn/patch/2449>
<http://www.cnvd.org.cn/patch/2450>
<http://www.cnvd.org.cn/patch/2451>

本周要闻速递

1. 微软表示 Word 可能被黑客利用 用户应警惕

微软于 12 月 28 日表示，黑客正在利用 Microsoft Word 中的漏洞攻击用户的 Windows 电脑。根据微软恶意软件保护中心公布的信息，恶意的攻击使用一种特别设计的 RTF 文件来进行，这种文件可以生成一个 Word 堆栈溢出，从而获取权限在用户主机上下载一个特洛伊木马并运行。微软在 Word 2007 和 2010 版本中评级该漏洞的时候使用了“危急”等级，而在其他 Office 版本中，这个漏洞被评级为“重要”，目前 Word 2002，2003，2007 和 2010 都受到影响，请广大用户尽快安装 11 月 9 日的安全补丁。

参考链接：<http://www.cnbeta.com/articles/131127.htm>

2. Skype Windows 客户端存在漏洞 导致大规模宕机

Skype 首席信息官于 12 月 29 日在官方博客中称，上周发生的大规模宕机事件是由于 Skype Windows 客户端漏洞所致。由于 Skype Windows 客户端（版本号为 5.0.0152）存在一处漏洞，致使多台负责处理离线消息的支持服务器超负荷运转，最终导致大规模宕机。Skype 首席执行官表示，最初，Mac 和 iPhone 用户并未受到影响，但由于 Windows 客户端故障未能及时解决，导致 Skype 整个服务系统最终崩溃。

参考链接：<http://tech.sina.com.cn/i/2010-12-29/23545042931.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