

信息安全漏洞周报

2011 年 1 月 3 日-2011 年 1 月 9 日

2011 年第 1 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 71 个，其中高危漏洞 12 个、中危漏洞 25 个、低危漏洞 34 个。上述漏洞中，可利用来实施远程攻击的漏洞有 65 个。经跟踪发现，网上已经出现针对“Microsoft Windows 'CreateSizedDIBSECTION()' 缩略图查看栈缓冲区溢出漏洞”、“Openfire 多个跨站脚本漏洞”、“Linux kernel 本地特权提升漏洞”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 40 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 产品存在安全漏洞

本周，Microsoft 发布安全公告称，Windows 绘图引擎存在一个“Microsoft Windows 'CreateSizedDIBSECTION()' 缩略图查看栈缓冲区溢出漏洞”。目前的漏洞分析情况表明，如果用户在以管理员权限使用操作系统时，攻击者可利用该漏洞在用户主机上执行特定构造的恶意代码、安装指定程序，并可以查看、修改、删除数据或创建拥有完全用户权限的新账户。如果仅以普通用户权限使用操作系统，则实时受到攻击的威胁较小。经过测试，目前受漏洞影响的 Windows 操作系统版本有 XP、Server 2003、Server 2008、Vista 等。微软已经发布了缓解性措施和临时修补文件来解决此漏洞。另外，Microsoft 还出现了“Microsoft Internet Explorer 'ReleaseInterface()' 远程代码执行漏洞”，攻击者可以利用这个漏洞在受影响的应用程序中运行任意代码。目前，微软尚未发布这个漏洞的修补程序，CNVD 提醒广大微软用户继续关注厂商主页，以获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03581>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03575>

2、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，攻击者可以利用漏洞发起恶意攻击，使内核崩溃、内存泄露并获取敏感信息。CNVD 本周收录的漏洞包括：Linux Kernel 本地特权提升漏洞、Linux Kernel 'hci_uart_tty_open()' 本地拒绝服务漏洞、Linux Kernel 'kvm_vcpu_events.interrupt.pad' 本地信息泄漏漏洞、Linux Kernel 'net/' 子系统套接字过滤器本地信息泄漏漏洞、Linux Kernel 'blk_rq_map_user_iov()' 本地拒绝服务漏洞。除“Linux Kernel 'kvm_vcpu_events.interrupt.pad' 本地信息泄漏漏洞”外，Linux 已经发布其余漏洞的修补程序，CNVD 提醒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-2011-03616>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03600>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03599>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03598>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03580>

3、MyBB 存在多个安全漏洞

MyBB 是一款免费 BBS 建站软件。本周，MyBB 产品出现了多个安全漏洞。攻击者可以利用这些漏洞实施拒绝服务或注入 WEB 脚本攻击，以获得用户权限或敏感信息。CNVD 收录的漏洞包括：MyBB 拒绝服务漏洞、MyBB 'member.php' 拒绝服务漏洞、MyBB 'usercp2.php' 跨站请求伪造漏洞、MyBB functions.php 文件任意帐号访问漏洞、MyBB 信息泄漏漏洞、MyBB 权限绕过漏洞、MyBB 跨站脚本攻击漏洞。目前，厂商已经发布了修补程序修复这些漏洞，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-2011-03631>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03630>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03629>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03628>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03624>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03623>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03622>

4、TIBCO Collaborative Information Manager 出现多个安全漏洞

TIBCO Collaborative Information Manager 软件是应用于企业的信息管理系统，主要用于企业多个业务单位、部门和合作伙伴协调企业的数据信息共享(如：产品、客户、供应商等信息)，并使这些信息与下游 IT 事务系统同步。本周，TIBCO Collaborative Information Manager 出现多个安全漏洞。CNVD 收录的漏洞包括：TIBCO Collaborative Information Manager 存在会话固定漏洞、TIBCO Collaborative Information Manager 存在信息泄露漏洞、TIBCO Collaborative Information Manager 存在跨站脚本漏洞、TIBCO Collaborative

Information Manager 存在多个 SQL 注入漏洞。攻击者可以利用这些漏洞劫持目标用户 WEB 会话、查看和修改敏感信息。目前，厂商已经发布了修补程序修复这些漏洞，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-2011-03619>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03618>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03617>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03615>

5、VLC Media Player Demuxer 存在远程拒绝服务漏洞

VLC Media Player 是一款多媒体播放器。本周，VLC Media Player 出现了一个远程拒绝服务漏洞，级别定义为“高危”。VLC Media Player 在处理 Real Media 文件中的畸形 Real demuxer 数组时存在索引错误，通过引诱用户打开特定构造的 Real Media 文件，远程攻击者可利用此漏洞使应用程序崩溃，甚至可以达到控制用户主机的目的。目前，厂商已发布该漏洞的补丁程序，CNVD 提醒广大用户及时下载更新，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-2011-03587>

小结：本周，Microsoft 发布了安全公告称，Windows 绘图引擎存在一个'CreateSizedDI BSECTION()'缩略图查看栈缓冲区溢出漏洞。攻击者可利用该漏洞在用户主机上执行特定构造的恶意代码、安装指定程序，并可以查看、修改、删除数据或创建拥有完全用户权限的新账户。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一定威胁。微软已经发布了缓解性措施和临时修补文件来解决此漏洞。此外，MyBB、TIBCO Collaborative Information Manager、Linux Kernel 和 VLC Media Player 均出现了多个安全漏洞。这些产品在国内用户中使用范围比较广泛，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、Apple 发布升级程序修补了“Apple Mac OS PackageKit 分发脚本远程代码执行漏洞”

Apple Mac OS X 是 Apple 公司发布的操作系统。本周，Apple 发布了最新 Mac OS X v10.6.6 版本，用于修复存在于 Mac OS X v10.6 至 v10.6.5 版本、Mac OS X Server v10.6 至 v10.6.5 版本中的“PackageKit 分发脚本远程代码执行漏洞”，以避免攻击者利用漏洞导致应用程序意外终止或执行任意指令。CNVD 已收录此补丁，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/2494>



本周要闻速递

1. 微软将于下周发布修复 Windows 漏洞的安全补丁

1月7日消息，微软将于下星期将发布两个安全补丁修复 Windows 的三个安全漏洞。其中一个补丁是微软最高级别的“严重”的补丁，另一个是“重要”级别的安全补丁。这两个补丁都将修复 Windows 中的安全漏洞。有安全专家表示，当中一个声称修复 Vista 漏洞的补丁令人感到困惑。这个东西也许只有 Vista 有，而在 Windows 7 系统中不存在，或者为 Windows 7 重新编写了。一些人推测这个安全漏洞也许存在于 Vista 系统的一个很少使用的组件中，如任务编排程序等。关于第二个安全补丁，微软没有提供更多的细节。

参考链接：<http://www.enet.com.cn/article/2011/0107/A20110107811754.shtml>

2、Microsoft Windows 绘图引擎存在零日漏洞 微软已发布缓解性措施和临时补丁

1月6日消息，微软宣布已经发布了缓解性措施和临时修补文件来解决 Windows 上出现的漏洞问题，并声称该漏洞对 Windows 7 操作系统和 Windows Server 2008 R2 服务器操作系统没有造成影响。此前，微软曾警告，包括 Vista, Server 2003 和 XP 系统在内的 Windows 图形处理机制出现了一个漏洞，且黑客将能利用该漏洞操纵用户的电脑。然而，微软表示目前尚未受到相关黑客的攻击。微软发言人表示，公司正着手研发更新的安全软件来解决该漏洞问题，并将与第三方以及微软主动防护计划(Microsoft Active Protections Program)的合作伙伴加强合作，以确保黑客无法利用漏洞建立恶意攻击性网站。

参考链接：http://news.ccidnet.com/art/946/20110106/2289023_1.html

3、谷歌称将尽快发布补丁修补短信功能的 BUG

1月8日消息，谷歌 Android 上周被曝出短信出现误发的现象，这可能要归咎于谷歌的开发人员。谷歌 Android 团队的一名成员在 Android 开源社区中表示，谷歌发现了两个致使短信功能出错的 BUG，其中一个会导致用户点击短信时显示错误的信息，另一个则会将短信错发给其他联系人。Android 项目成员表示，谷歌需要时间来处理这个问题，因为这个问题好像很少发生。开发人员需要再现这种情况，然后开发出相应的补丁。

参考链接：http://news.ccidnet.com/art/1032/20110108/2291081_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