

信息安全漏洞周报

2011 年 7 月 11 日-2011 年 7 月 17 日

2011年第28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 100 个，其中高危漏洞 37 个、中危漏洞 56 个、低危漏洞 7 个。上述漏洞中，可利用来实施远程攻击的漏洞有 75 个。网上已经出现针对“Dell OpenManage IT Assistant 'detectIESettingsForITA.OCX'信息泄露漏洞”、“Freefloat FTP Server 'LIST'命令远程缓冲区溢出漏洞”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。本周收录的漏洞中，已有 52 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。

成员单位报送漏洞统计

本周，4 家成员单位和浪潮集团报送了本周收录的全部 100 个漏洞，各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技、恒安嘉新报送的数量较多。

报送单位或个人	漏洞报送数量	私有漏洞数量
启明星辰	60	0
绿盟科技	45	0
恒安嘉新	44	0
安氏领信	4	0
浪潮集团	4	4
总计	100（去重）	4

表 1 成员单位上报漏洞统计表

本周，CNVD 整理和发布的漏洞涉及 Microsoft、Trend Micro、VideoLAN、Linux、Dell 等多家厂商的产品，漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Microsoft	21	21%
2	Transparent	7	7%

	Technologies		
3	Trend Micro	3	3%
4	libpng	3	3%
5	SquirrelMail	3	3%
6	VideoLAN	2	2%
7	Joomla!	2	2%
8	Linux	2	2%
9	Dell	1	1%
10	Symantec	1	1%
11	其他	55	55%

表 2 漏洞产品涉及厂商分类统计

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 产品安全漏洞

本周，微软发布了 2011 年 7 月份的月度例行安全公告，包含 4 项安全更新。其中，1 项更新的综合评级为“严重”，此项更新修复了一个秘密报告的 Windows 蓝牙堆栈漏洞。攻击者可以利用漏洞远程执行任意代码，随后执行安装程序，查看、更改或删除数据或者创建拥有完全相同用户权限的新帐户。受影响的操作系统平台涉及 Windows 7 和 Vista。另外 3 项更新的综合评级为“重要”，修复了涉及 Windows 7，XP，Vista 和 Server 2003/2008 的权限提升漏洞以及 Office Visio 组件存在的远程代码执行漏洞。CNVD 收录的相关漏洞包括：Microsoft Windows win32k.sys 驱动空指针错误应用漏洞（CVE-2011-1888、CVE-2011-1887、CVE-2011-1885、CVE-2011-1881、CVE-2011-1880）、Microsoft Windows win32k.sys 驱动内存错误引用漏洞（CVE-2011-1884、CVE-2011-1883、CVE-2011-1882、CVE-2011-1876、CVE-2011-1879、CVE-2011-1878、CVE-2011-1877、CVE-2011-1875、CVE-2011-1874）、Microsoft Windows CSRSS 特权提升漏洞（CVE-2011-1870、CVE-2011-1284、CVE-2011-1283、CVE-2011-1282、CVE-2011-1281）、Microsoft Windows 蓝牙栈'btport.sys'驱动远程代码执行漏洞。其中，“Microsoft Windows win32k.sys 驱动内存错误引用漏洞（CVE-2011-1875、CVE-2011-1874）、Microsoft Windows 蓝牙栈'btport.sys'驱动远程代码执行漏洞”的综合评级为“高危”。CNVD 提醒广大 Microsoft 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-2011-06272>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06271>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06270>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06269>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06268>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06267>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06265>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06264>

2、Cisco VPN 客户端权限提升漏洞

Cisco VPN Client 是 Cisco 的虚拟专用网络 (VPN) 客户端软件。本周，基于 64 位 Windows 7 平台的 Cisco VPN 客户端存在一个本地特权提升漏洞，允许非特权用户获得管理权限。目前，Cisco 已经发布升级程序修补这个漏洞，CNVD 提醒广大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-2011-06225>

3、Symantec Web Gateway 管理接口 SQL 注入漏洞

Symantec Web Gateway 是一款 Web 安全网关硬件设备。本周，Symantec Web Gateway 被披露存在一个 SQL 注入漏洞。由于通过 "username" 参数传递给管理接口中的 forget.php 的输入在用于 SQL 查询之前缺少过滤，攻击者可以通过 SQL 注入攻击获得敏感信息或操作数据库。该漏洞的综合评级为“高危”。目前，Symantec 已经发布升级程序修补这个漏洞，CNVD 提醒广大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-2011-06221>

4、libpng 产品安全漏洞

libpng 是一款多种应用程序所使用的解析 PNG 图形格式的函数库。本周，libpng 被披露存在多个安全漏洞，攻击者可以利用这些漏洞触发缓冲区溢出，导致应用程序崩溃或拒绝服务。CNVD 收录的漏洞包括：libpng 拒绝服务漏洞(CVE-2011-2691)、libpng 缓冲区溢出漏洞(CVE-2011-2690)、libpng PNG 文件拒绝服务漏洞。上述漏洞中，“libpng 缓冲区溢出漏洞(CVE-2011-2690)”的综合评级为“高危”。目前，厂商已经发布这些漏洞的补丁程序，CNVD 提醒广大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-2011-06283>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06288>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-06290>

5、Dell OpenManage IT Assistant 'detectIESettingsForITA.OCX'信息泄露漏洞

Dell OpenManage IT Assistant 可用于查找和提供各种 DELL 系统的信息摘要。本周，Dell OpenManage IT Assistant 被披露存在一个信息泄露漏洞。由于 Dell OpenManage IT Assistant 'detectIESettingsForITA.OCX'控件不安全使用 "readRegVal()" 方法，允许攻击者查询目标用户系统上的注册表键值，获得敏感注册表值信息。目前，互联网上已经出现

针对该漏洞的攻击代码，主要影响 Dell OpenManage ITAssistant 8.9.0 版本。厂商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获取最新版本。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2011-06311>

小结：本周，Microsoft 发布 2011 年 7 月安全公告，修补多个产品安全漏洞，远程或本地攻击者可以利用漏洞提升特权或执行任意代码，对使用微软产品的用户构成较为严重的威胁。同时，Cisco VPN 客户端、Symantec Web Gateway 和 libpng 产品也被披露存在多个安全漏洞。此外，Dell OpenManage IT Assistant 零日漏洞也对使用该产品的用户构成较大威胁。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、Apache 发布升级程序，修补 Tomcat 安全漏洞

本周，Apache 发布升级程序，修补了 Tomcat 存在的多个安全漏洞。本地攻击者可以利用漏洞绕过安全限制或使 JVM 崩溃。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/4406>

本周要闻速递

1. Skype 被披露存在安全漏洞

据国外媒体报道，德国一名安全专家周三在网上公布了网络电话服务软件 Skype 存在的一个“重大安全漏洞”，称恶意攻击者可借此劫持用户密码。Skype 这个安全漏洞源于跨网站代码错误，即用户在使用 Skype 服务之前，必须首先输入手机号码和密码。而利用 Skype 的这个安全漏洞，恶意攻击者可在要求用户输入手机号码的区域插入 JavaScript 代码。如此一来，恶意攻击者其他联系人上线后，相应 JavaScript 代码将被自动执行，恶意攻击者将可查看该联系人的登录信息，并有可能通过该方式劫持该联系人的电脑，同时可借此更改 Skype 用户帐号的密码。安全专家建议，Skype 应该对用户输入手机号码区域进入检查，以确保该区域不被插入可执行代码。他表示，该漏洞存在于 Skype 最新 5.3.0.120 版本当中，Windows XP、Vista、Windows 7 及 Mac OS X 等操作系统用户皆受到影响。

参考链接: <http://tech.qq.com/a/20110716/000098.htm>

2. 通信公司推出安全更新保护黑莓企业服务器

据国外媒体报道，日前加拿大通信公司推出一个安全更新来保护黑莓企业服务器

（BES）平台不受管理员 API 组件漏洞的影响，该漏洞会导致服务器被临时离线。攻击者能够利用该漏洞执行拒绝服务攻击或者获取系统信息。该更新可以安装在运行 BES5.0.3 及以前版本的所有系统中，同时也包括 BES Lite 和微软的 Exchange，IBM Lotus Domino 和 GroupWise 版本的服务器平台。现在该更新已经可以从该通信公司的服务器上下载，管理员可以通过在隔离网络中运行 BES 来减轻攻击所带来的潜在影响。该公司提醒称，该漏洞不会影响黑莓手持设备，平板电脑或者非 BES 的软件平台。

参考链接：http://news.ccidnet.com/art/951/20110717/2438991_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