

信息安全漏洞周报

2011 年 9 月 5 日-2011 年 9 月 11 日

2011 年第 36 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**高**。

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 110 个，其中高危漏洞 47 个、中危漏洞 54 个、低危漏洞 9 个。上述漏洞中，可利用来实施远程攻击的漏洞有 97 个。网上已经出现针对“Microsoft Windows stdout/stdin 本地拒绝服务漏洞”、“Crush FTP 'APPE'命令远程拒绝服务漏洞”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 45 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，共 6 家成员单位报送了本周收录的全部 110 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	73	0
绿盟科技	64	0
恒安嘉新	63	0
安天	6	0
安氏领信	3	0
东软	3	0
总计	110（去重）	0

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 WordPress、Wireshark、Linux、IBM、Apple 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	WordPress	15	13.6%

2	Mambo	7	6.3%
3	Wireshark	4	3.6%
4	Linux	3	2.7%
5	Advantech	3	2.7%
6	OpenTTD	3	2.7%
7	IBM	2	1.8%
8	Cisco	2	1.8%
9	Apple	2	1.8%
10	Microsoft	2	1.8%
11	其它	67	61.2%

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 Windows 安全漏洞

Microsoft Windows 是一款流行的操作系统。本周，Microsoft Windows 被披露存在多个安全漏洞。远程或本地攻击者可以利用漏洞以用户安全上下文执行任意代码或进行拒绝服务攻击。CNVD 收录的相关漏洞包括：Microsoft Windows stdout/stdin 本地拒绝服务漏洞、Microsoft Windows Script Host 'wshehn.dll' DLL 装载任意代码执行漏洞。其中，“Microsoft Windows Script Host 'wshehn.dll' DLL 装载任意代码执行漏洞”的综合评级为“高危”。目前，互联网上已经出现针对“Microsoft Windows stdout/stdin 本地拒绝服务漏洞”的攻击代码，影响 Windows Server 2008 多个版本。微软尚未发布上述漏洞的修补程序，CNVD 提醒 Microsoft 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-2011-07186>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07112>

2、IBM 产品安全漏洞

IBM OpenAdmin Tool for Informix 是一款 GUI 管理工具；IBM Java SDK 是 Java 语言开发环境。本周，上述 IBM 产品存在多个安全漏洞。攻击者可以利用漏洞在受影响站点上下文的浏览器会话中执行任意 HTML 和脚本代码或造成拒绝服务攻击。CNVD 收录的漏洞包括：IBM OpenAdmin Tool for Informix 存在多个跨站脚本漏洞、IBM Java 类文件解析拒绝服务漏洞。目前，IBM 已经发布上述漏洞的补丁程序，CNVD 提醒广大 IBM 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-2011-07189>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07182>

3、Apple 产品安全漏洞

本周，Apple 的产品 QuickTime 播放器和 Mac OS X 操作系统被披露存在漏洞，攻击者可以利用漏洞绕过安全限制或以应用程序上下文执行任意代码。CNVD 收录的相关漏洞包括：Apple QuickTime 'QuickTimePlayer.dll' ActiveX 缓冲区溢出漏洞、Apple Mac OS X 密钥串证书设置安全绕过漏洞。其中，“Apple QuickTime 'QuickTimePlayer.dll' ActiveX 缓冲区溢出漏洞”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 Apple QuickTime Player 7.6.9 版本。Apple 尚未发布上述漏洞的补丁程序，CNVD 提醒广大用户随时关注厂商主页以获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07148>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07100>

4、WordPress 插件安全漏洞

WordPress 是一款使用 PHP 语言开发的 Web 内容管理系统(CMS)。本周，WordPress 多款插件被披露存在多个安全漏洞，攻击者可以利用漏洞访问或修改数据，或进一步利用底层数据库中潜在的漏洞。CNVD 收录的相关漏洞包括：WordPress KNR Author List Widget 'listItem'参数 SQL 注入漏洞、WordPress 插件 Post Highlights 'ph_settings.php' SQL 注入漏洞、WordPress 插件 VideoWhisper 'c_status.php' SQL 注入漏洞、WordPress 插件 DukaPress Shopping Cart 任意文件上传漏洞、WordPress 插件 Facebook Open Graph Meta 'all_meta.php' SQL 注入漏洞、WordPress 插件 oQey Gallery 'ga_id'参数 SQL 注入漏洞、WordPress 插件 Zotpress 'zotpress.rss.php' SQL 注入漏洞、WordPress 插件 iCopyright(R) Article Tools 'id'参数 SQL 注入漏洞。上述漏洞的综合评级均为“高危”，且部分漏洞的攻击代码已在互联网出现。目前，除“WordPress 插件 DukaPress Shopping Cart 任意文件上传漏洞”外，厂商尚未发布其余漏洞的补丁程序，CNVD 提醒广大 WordPress 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-2011-07174>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07173>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07165>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07149>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07141>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07135>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07134>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07122>

5、Cisco 产品安全漏洞

本周，Cisco 的产品 Nexus 系列交换机、NX-OS 操作系统存在多个安全漏洞，攻击者可以利用漏洞访问设备上运行的操作系统或导致拒绝服务。CNVD 收录的相关漏洞包

括：Cisco Nexus 5000 和 3000 系列交换机 ACL 安全绕过漏洞、Cisco NX-OS CDP Packety 远程堆内存破坏漏洞。上述漏洞中，“Cisco NX-OS CDP Packety 远程堆内存破坏漏洞”的综合评级为“高危”，且互联网上已经出现针对该漏洞的攻击代码，影响 Cisco NX-OS 多个版本。厂商尚未发布该漏洞的补丁程序，只发布了“Cisco Nexus 5000 和 3000 系列交换机 ACL 安全绕过漏洞”的补丁，CNVD 提醒广大 Cisco 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-2011-07177>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-07169>

小结：本周，Microsoft Windows 被披露多个安全漏洞，远程或本地攻击者可以利用漏洞以用户安全上下文执行任意代码或进行拒绝服务攻击，对使用 Windows 的用户构成较为严重的威胁。此外，CNVD 还收录了 IBM、Cisco、Apple 产品和 Wordpress 插件的多个漏洞。Cisco NX-OS CDP Packety 远程堆内存破坏漏洞、Microsoft Windows stdout/stdin 本地拒绝服务漏洞和 Apple QuickTime 'QuickTimePlayer.dll' ActiveX 缓冲区溢出漏洞为 0day 漏洞，攻击代码已在互联网上出现，有可能引发互联网上的大规模网络攻击事件。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、OpenSSL 发布升级程序，修补 多个安全漏洞

OpenSSL 是一款开放源码的 SSL 应用软件，用来实现网络通信的高强度加密。OpenSSL ephemeral ECDH 加密实现存在错误，攻击者以不正确序列发送握手消息可使目标服务器崩溃。要成功利用漏洞需要服务器启用和支持 ECDH 加密。此外，ECDH 实现为非线程安全。目前，供应商发布了安全公告及相关补丁信息，修复了此漏洞。

补丁下载链接：<http://www.cnvd.org.cn/patch/5007>

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周要闻速递

1. 微软将修复 15 个安全漏洞

据国外媒体报道，微软周四称，它将在下周二发布 5 个安全补丁，修复 Windows、Excel、SharePoint Server 和 Groove 等软件中的 15 个安全漏洞。所有这 5 个安全补丁都是

“重要”等级的。有两个补丁修复 Windows 的安全漏洞，其中 1 个补丁仅修复服务器版的安全漏洞，如 Server 2003、Server 2008 和 Server 2008 R2。第二个补丁修复所有支持版本的 Windows 操作系统，包括已有 10 年之久的 XP 和比较新的 Windows 7。另外两个补丁修复 Excel 软件中的安全漏洞，包括最新的 Windows 版 Excel 2010 和 Mac 版 Excel 2011 以及 Office 软件中的 Excel。第五个补丁修复各种服务器方面的软件中安全漏洞，包括 SharePoint、Groove 和 Office Web Apps 等软件中的安全漏洞。安全人员指出，虽然微软发布的补丁中有三个安全漏洞能够被攻击者用于远程执行代码，也就是劫持用户的计算机，但是微软为这些安全补丁提供的安全等级表明，攻击者需要在用户的参与下才能利用这些安全漏洞，如欺骗用户访问一个恶意网站等。

参考链接: http://news.ccidnet.com/art/11099/20110909/2733441_1.html

2. QQ 群曝出安全漏洞并被黑客利用

最近有消息称，QQ 群共享功能曝出安全漏洞，并被黑客利用制作蠕虫病毒，目前日均感染两万多台 QQ 用户电脑。据杀毒扫描网站显示，该蠕虫病毒最早在 8 月 24 日已在网上公开出现，而腾讯公司也公开回应表示，QQ 安全团队于 9 月 5 日晚间发现了此类蠕虫，并开始着手修复漏洞。据悉，QQ 群蠕虫病毒一般伪装为“电视棒升级破解版”，诱骗网民点击使用，借机感染用户电脑。一旦有一台电脑中招，该蠕虫病毒就会自动上传到中招者的 QQ 群共享里，对 QQ 群中其他网友造成威胁，伺机窃取 QQ 账号等重要信息。网络安全机构提示，通过 QQ 群共享下载文件时，应确保电脑开启有效的安全软件，保护账号不被黑客窃取，而不是被病毒感染了再事后补救。

参考链接: <http://it.people.com.cn/h/2011/0906/c227888-3548367671.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