

信息安全漏洞周报

2010 年 11 月 1 日-2010 年 11 月 7 日

2010 年第 43 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 94 个，其中高危漏洞 15 个、中危漏洞 38 个、低危漏洞 41 个。上述漏洞中，可利用来实施远程攻击的漏洞有 83 个。经跟踪发现，网上已经出现针对“Maxthon 浏览器 CSS 远程拒绝服务漏洞”、“Android 2.0-2.1 下 Webkit 缺陷引发的反弹 Shell 漏洞”以及“Microsoft Internet Explorer CSS 标签远程代码执行漏洞”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 75 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 多款产品存在安全漏洞

Microsoft Data Access Objects (DAO)数据访问对象是一种应用程序编程接口。本周，CNVD 收录了 Microsoft Data Access Objects (DAO) 'dao360.dll' DLL 装载任意代码执行漏洞和 Microsoft Internet Explorer CSS 标签远程代码执行漏洞。其中“Microsoft Internet Explorer CSS 标签远程代码执行漏洞”为 0day 漏洞，互联网上已经出现针对 IE 6 和 IE 7 的漏洞攻击程序。攻击者可以利用这些漏洞获取敏感信息、执行任意代码或发起拒绝服务攻击等。目前微软尚未提供漏洞解决方案，CNVD 提醒广大用户继续关注相关厂商发布的安全公告信息，以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-2010-02666>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02725>

2、Linux 存在多个安全漏洞

Linux 是一款开放源代码的操作系统。本周，linux 出现多个安全漏洞，CNVD 收录的 linux 安全漏洞包括：Linux 内核 RDS 协议本地整数溢出漏洞、Linux 下的 HP Insight Control

跨站请求伪造漏洞、Linux-PAM pam_namespace 模块本地权限提升漏洞、Linux 内核'net/'子系统本地信息泄漏漏洞等，其中“Linux 内核 RDS 协议本地整数溢出漏洞”的漏洞等级为“高危”。CNVD 提醒广大用户继续关注相关厂商发布的更新信息并及时下载更新，以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-2010-02660>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02654>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02720>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02723>

3、Adobe存在多个安全漏洞

Adobe Shockwave Player 是专门播放使用Director Shockwave Studio制作的网页的外挂软件。CNVD本周收录的Adobe Shockwave Player漏洞包括：Adobe Shockwave Player 'IML32.dll'文件缓冲区溢出漏洞、Adobe Shockwave Player 'dirapi.dll'文件缓冲区溢出漏洞、Adobe Shockwave Player未明缓冲区溢出漏洞、Adobe Shockwave Player未明堆缓冲区溢出漏洞。攻击者可以利用上述漏洞执行任意代码、破坏内存或者发起拒绝服务攻击。其中“Adobe Shockwave Player 'IML32.dll'文件缓冲区溢出漏洞”和“Adobe Shockwave Player 未明缓冲区溢出漏洞”等的漏洞等级为“高危”，厂商已发布了这些漏洞的升级补丁以修复这些漏洞，建议广大Adobe用户及时下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02727>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02729>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02739>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02746>

4、Android 2.0-2.1下Webkit缺陷引发的反弹Shell漏洞

Android系统下基于Webkit内核的手机浏览器存在一个倾向于远程代码执行的漏洞，当WebKit处理浮点数据类型时存在输入验证漏洞，访问恶意网站会导致浏览器意外终止或执行任意代码。远程攻击者可利用此漏洞进行缓冲区溢出，导致执行任意代码，如果溢出失败则可能引起拒绝服务。目前Webkit官方已经修补了此漏洞。建议采用新版Webkit内核的手机浏览器或使用其他内核的手机浏览器来防止此漏洞的影响。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02749>

5、ProFTPD产品存在安全漏洞

ProFTPD是一款Unix平台上或是类Unix平台上的FTP服务器软件。该软件存在多个安全漏洞，CNVD本周收录了“ProFTPD函数缓冲区溢出漏洞”和“ProFTPD模块目录遍历漏洞”。ProFTPD的mod_site_misc模块中存在多个输入验证错误，攻击者可以通过目录遍历攻击写入或删除任意目录、创建符号链接或更改文件时间。ProFTPD的src/netio.c文件中的pr_netio_telnet_gets()函数在处理包含有Telnet IAC转义序列的用户输入时存在栈溢出，远程攻击者可以通过向FTP或FTPS服务提交恶意输入进而执行任意代码。厂商已发布了升级补丁修复这些安全漏洞，CNVD建议用户关注厂商主页以获得修补方案。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02715>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02714>

6、HP多款产品存在安全漏洞

本周，CNVD收录了HP多款产品存在的多个漏洞。其中较为重要的漏洞包括：HP Insight Control Performance Management未明权限提升漏洞、HP Storage Essentials LDAP认证未明漏洞、HP LoadRunner Web Tours未明漏洞、HP Palm webOS摄像应用程序未明漏洞、HP Palm webOS服务'API'未明漏洞、HP Insight Control Power Management未明跨站请求伪造漏洞、HP Insight Control Power Management未明跨站脚本攻击漏洞、HP Insight Control Virtual Machine Management未明跨站脚本攻击漏洞、HP Insight Control Virtual Machine Management未明跨站请求伪造漏洞、HP Insight Control Performance Management未明跨站脚本攻击漏洞、HP Palm webOS 'Doc Viewer'未明漏洞。受这些漏洞影响的相关产品包括：HP palm webos 1.4.1、HP loadrunner web tours 9.10、HP loadrunner <=9.1、HP storage essentials <=6.2、HP insight control power management <=6.1.2、HP Insight Control virtual machine management <=6.1.2。攻击者可以利用这些漏洞借助未明向量注入任意web脚本或者HTML、获取特权、劫持用户认证过程，获取敏感信息，修改数据或者发起拒绝服务攻击。攻击者如获得本地用户权限，还可以利用执行某些服务调用的功能获取更高权限，并对系统文件进行覆盖操作。目前厂商已经发布了升级补丁以修复上述安全问题，CNVD建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02696>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02695>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02694>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02693>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02692>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02691>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02711>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02738>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02737>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02712>

小结：本周，微软于11月3日发布了关于Microsoft Internet Explorer CSS 标签远程代码执行零日漏洞的安全公告，该漏洞存在于浏览器IE的6.0、7.0和8.0版本中，并已出漏洞攻击程序，CNVD已发布安全公告并提供了临时解决方案。此外，HP、ProFTPD、Linux、Android系统、Adobe等应用广泛的产品均出现了安全漏洞，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、Python 发布漏洞修补更新程序

Python 是一款面向对象、直译式计算机程序设计语言。本周，Python 被发现存在安全漏洞，允许攻击者进行拒绝服务攻击。SMTPChannel 类的"__init__()"方法存在竞争条件错误，可导致进程崩溃。此外，SMTPServer 类的"handle_accept()"方法存在错误，可导致进程崩溃。目前，厂商已经发布了上述漏洞的修复升级程序，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/1551>

本周要闻速递

1、Android 内核存在大量高风险漏洞

美国软件分析公司 Coverity 本周宣布，Android 内核中存在大量漏洞，其中包括 88 个高风险漏洞，有可能导致用户敏感信息泄露。该公司对 2.6.32 版本的 Android 操作系统内核进行分析，宏达电 Droid Incredible 等手机均采用该系统。结果显示，该系统存在 359 个软件漏洞，其中 25% 被认定为高风险漏洞，有可能导致安全问题和系统崩溃。Coverity 已经向谷歌和宏达电通知了上述 Android 漏洞。如果得到证实，这些漏洞将会通过无线升级进行修复。

参考链接：<http://safe.zol.com.cn/202/2028828.html>

2、PayPal 提供更新修补 iPhone 漏洞

互联网支付服务提供商 PayPal 表示，它已经向用户提供更新，以修补 iPhone 版本的安全漏洞，该漏洞能使黑客拦截到用户的密码。更新程序修补的漏洞只会影响使用不安全 WIFI 网络连接的 iPhone 用户，Android 版本和访问 PayPal.com 网站的用户均不受影响。漏洞会导致程序无法验证 PayPal 的数字证书。一旦无法确认，黑客就可以假扮成 PayPal 网站，窃取用户的账号和密码。不过漏洞需要黑客与用户在同一地方，使用相同的 WIFI 网络，这就意味着黑客可能会利用车站等公共 WIFI 热点，窃取使用 iPhone 版 PayPal 交易的用户信息。Paypal 发言人阿曼达·皮雷斯表示，公司已经将新版的 Paypal 程序上传至苹果 App Store，用户可自行下载。

参考链接：http://www.infosec.org.cn/news/news_view.php?newsid=13940

3、微软 11 月安全公告预告：3 个补丁 修复 11 处漏洞

微软 11 月 5 日发布了 11 月份安全公告预告，计划在 11 月 9 日发布本月例行补丁。继上月微软创纪录发布了 16 个安全补丁，修复了多达 49 个安全漏洞之后，本月微软计划发布 3 个补丁，修复 11 个漏洞。在本月即将发布的 3 个安全补丁中，只有 1 个为最高的危急级别，另外 2 个为重要级别。这 3 个补丁中有两个涉及 Office，另外一个补丁则将修复 Forefront Unified Access Gateway 中的一个权限提升漏洞。

参考链接：<http://tech.sina.com.cn/s/2010-11-05/09374832391.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