

信息安全漏洞周报

2010 年 11 月 22 日-2010 年 11 月 28 日

2010 年第 46 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 46 个，其中高危漏洞 5 个、中危漏洞 8 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 27 个。经跟踪发现，网上已经出现针对“Microsoft Windows 内核计划任务服务本地特权提升漏洞”、“Apache Tomcat 'sort'参数跨站脚本漏洞”、“ZyXEL P-660R-T1 V2 'HomeCurrent_Date'参数跨站脚本漏洞”以及“Microsoft Windows 用户访问控制绕过本地特权提升漏洞”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 31 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、Linux Kernel 出现多个安全漏洞

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，本地攻击者能够利用漏洞获得敏感信息。CNVD 本周收录的相关漏洞包括：Linux Kernel 'hmid_ds structure'本地信息泄漏漏洞、Linux Kernel 'hdsp.c' IOCTL 本地信息泄漏漏洞、Linux Kernel 'SNDRV_HDSP_IOCTL_GET_CONFIG_INFO' IOCTL 本地信息泄漏漏洞、Linux Kernel TIOCGICOUNT CVE-2010-4077 本地信息泄漏漏洞、Linux Kernel 'FBIOGET_VBLANK' IOCTL 本地信息泄漏漏洞、Linux Kernel 套接字拒绝服务漏洞、Linux Kernel 'inotify_init()'内存泄漏本地拒绝服务漏洞。目前 Linux 已经发布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-2010-03023>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03022>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03021>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03020>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03019>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03018>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03010>

2. Apple 产品存在多个安全漏洞

本周，Apple 的 iOS 系统和 Safari 浏览器存在多个安全漏洞。Apple iOS 是一款运行在苹果 iPhone 和 iPod touch 设备上的操作系统。Safari 是苹果家族操作系统捆绑的 WEB/WAP 浏览器。CNVD 收录的相关漏洞包括：Apple Safari WebKit 权限许可和访问控制漏洞、Apple iOS 照片处理安全绕过漏洞、Apple iPhone/iPod/iPad 配置文件签名验证绕过漏洞、Apple iOS iAd 内容显示 URL 机制处理安全绕过漏洞、Apple iOS 网络报文过滤器规则本地特权提升漏洞、Apple iOS 电话基带处理器堆缓冲区溢出漏洞。攻击者会利用这些漏洞注入恶意代码，获得系统权限。其中“Apple Safari WebKit 权限许可和访问控制漏洞”的安全等级为“高危”。目前，厂商已经发布升级补丁修复这些安全漏洞，CNVD 建议广大 Apple 用户及时下载更新，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-2010-03032>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02998>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02997>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02996>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02995>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02994>

3、Cisco 存在安全漏洞

Cisco Unified Videoconferencing 是思科统一通信系统的重要组件，用于构建一个可靠、便于管理、经济有效的视频会议应用网络环境，广泛用于互联网企业和电信运营商中。本周 Cisco UVC System 出现了多个安全漏洞，攻击者可以利用漏洞获得敏感信息或进行会话劫持，CNVD 本周收录的相关漏洞包括：Cisco UVC System 多个产品 Config/Mcu.val 文件加密问题漏洞、Cisco UVC System 多个产品/etc/shadow 文件信任管理漏洞、Cisco UVC System 多个产品 web 接口授权问题漏洞、Cisco UVC System 产品 web 接口信息泄露漏洞。目前，漏洞厂商还没有提供此漏洞的相关补丁或者升级程序，CNVD 提醒使用此软件的用户随时关注厂商的主页以获取最新版本，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-2010-03039>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03038>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03037>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03008>

4、Microsoft Windows 存在多个安全漏洞

Microsoft Windows 是微软开发的操作系统系列产品。本周，包括：Windows 7、Vista、server 2008 的多个版本 Windows 操作系统被发现存在“用户访问控制绕过本地特权提升漏洞”和“内核计划任务服务本地特权提升漏洞”。本地攻击者利用这些漏洞能够进行执行

任意代码攻击以及系统权限获取。目前微软还没有提供此漏洞的修补程序，CNVD 提醒广大微软用户随时关注厂商的主页以获取最新版本，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-2010-03011>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-03002>

5. Symantec PGP Desktop 存在安全漏洞

Symantec PGP Desktop 是一款功能强大的加密签名工具。本周，Symantec PGP Desktop 被披露存在一个消息验证错误漏洞。当接收者右键解密和校验.pgp 文件时，PGP Desktop 会输出加密数据，并在验证后报告完全合法。利用该漏洞，攻击者可以通过截获签名的 OpenPGP 消息，将未签名的数据插入到受信任的消息中，达到攻击目的。该漏洞存在于 Symantec PGP Desktop 10.0.3 之前版本以及 10.0.1 版本中。目前，厂商已经发布了安全公告及相关补丁信息，修复了此漏洞，建议用户及时下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02992>

小结：本周，Apple 发布 iOS 4.2 修复了多个漏洞，同时 Apple 还发布了 Apple TV 4.1，修复了 FreeType 和 libpng 的多个漏洞。此外，微软、Linux、Cisco 等厂商产品均出现了多个安全漏洞，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、Wireshark 发布升级程序修补了 2 个重要漏洞

Wireshark 是一款开放源代码的网络协议分析工具。Wireshark 处理部分协议时存在安全问题，远程攻击者可以利用漏洞对目标用户进行拒绝服务攻击或执行任意代码。epan/dissectors/packet-ldss.c 中的“dissect_ldss_transfer()”函数存在边界条件错误，可导致基于堆的缓冲区溢出，此漏洞存在于 1.2.0 至 1.2.12 版，及 1.4.0 至 1.4.1 版中。此外，在 ZigBee ZCL 发现属性应答解析中也存在一个漏洞，可造成死循环导致拒绝服务攻击，此漏洞存在于 1.4.0 至 1.4.1 版中。Wireshark 1.4.2 或者 1.2.13 已经修复上述漏洞，建议 Wireshark 用户尽快下载使用。

补丁参考链接：<http://www.cnvd.org.cn/patch/1858>

本周要闻速递

1.微软证实 Win7 存在 0day 漏洞可绕过 UAC

微软证实，他们正在调查一个关于 Windows 的 0-day 漏洞。据报道，32 位和 64 位的 Windows XP、Windows Vista 和 Windows 7 系统都受此漏洞的影响。恶意软件技术专家 Marco

Giuliani 指出：“这是一个非常严重的问题，因为它存在于 win32k.sys，是 Windows 子系统的内核模式部分。它是一个权限提升漏洞，被利用后，各类账户都能在内核模式中执行任意代码。” 由于该漏洞是权限提升漏洞，攻击者可以利用它绕过 Vista 和 Windows 7 中的用户账户控制（UAC）和受限用户账户（LUA）。所幸的是，该漏洞暂时还未能被利用发动远程攻击。

参考链接：<http://it.sohu.com/20101126/n277935111.shtml>

2. Android 2.3 将修复一个数据窃取漏洞

Android 2.3 系统近期将修复现有系统中的一个数据窃取漏洞。谷歌 Android 安全小组目前正在着手修补浏览器数据窃取漏洞，这个漏洞可以使网站未经授权就可以访问 Android 设备内存卡中的存储文件。漏洞最先由托马斯·坎农（Thomas Cannon）发现，他表示，自动文件下载、JavaScript 和 MicroSD 访问政策加在一起，在浏览器或电子邮件中点击某些 HTML 页面，用户的隐私数据可能会被窃取。不过这个漏洞实现起来要有特定条件，关键是第三方必须知道他们想偷窃的文件名称。由于许多 Android 设备都遵循照片和视频文件的标准化命名方式，窃取方可能也找不到什么。在手机升级到 Android2.3 系统前，建议用户要警惕可疑网站、电子邮件中的 HTML 链接或 Android 通知栏中突然弹出的下载。

参考链接：<http://www.hackbase.com/news/2010-11-25/39679.html>

3. 苹果公司正式发布苹果 iOS4.2，修复了以前版本存在的多个漏洞

据国外媒体消息，苹果公司于美国时间 11 月 22 日上午 7 点正式对外发布了 iOS4.2 升级系统，iPhone、iPod Touch 和 iPad 用户从即日起可对自己的爱机进行升级。这一款新系统的推出可谓是万众瞩目，它将较之前发布的 iOS4.2 系统更进一步，为 iPhone、iPod Touch 以及 iPad 增加更多的性能。iPad 用户在将系统升级至 iOS4.2 之后，就能够进行多任务操作，建立文件夹来整理应用程序，并且能够更加简便地从一个邮箱转登到另一邮箱。iOS4.2 系统适用于 iPhone3G，iPhone3GS 和 iPhone4；iPod Touch2G，Touch3G 和 Touch4G 以及 iPad。要升级至 iOS4.2 系统首先需要将你的 iTunes 升级到苹果公司上周发布的 10.1 版本。

参考消息：<http://gb.cri.cn/30524/2010/11/23/5291s3065166.htm>

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