

信息安全漏洞周报

2010 年 11 月 15 日-2010 年 11 月 21 日

2010 年第 45 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 104 个，其中高危漏洞 28 个、中危漏洞 29 个、低危漏洞 47 个。上述漏洞中，可利用来实施远程攻击的漏洞有 86 个。跟踪发现，网上已经出现针对“CMNC-200 IP 摄像机存在拒绝服务攻击漏洞”、“Camtron CMNC-200 ActiveX 控件缓冲区溢出漏洞”以及“VLC 媒体播放器错误调用转换栈破坏漏洞”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 85 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、IBM 多款产品存在安全漏洞

本周，IBM 的 OmniFind、WebSphere 和 Systems Director 等多款产品出现了安全漏洞。CNVD 收录的该产品的漏洞包括：IBM Systems Director 权限许可和访问控制漏洞、IBM Systems Director Agent reset_diragent_keys 不安全文件权限漏洞、IBM OmniFind 跨站脚本攻击漏洞、IBM WebSphere MQ 加密问题漏洞、IBM WebSphere MQ FDC 处理拒绝服务漏洞、IBM WebSphere MQ 拒绝服务漏洞、IBM OmniFind 管理员界面授权问题漏洞、IBM OmniFind 登陆表单缓冲区溢出漏洞、IBM OmniFind ESSearchApplication 树形目录授权问题漏洞、IBM OmniFind ESSearchApplication/palette.do 文件信任管理漏洞、IBM OmniFind 权限许可和访问控制漏洞、IBM OmniFind 资源管理错误漏洞、IBM OmniFind estaskwrapper 非信任搜索路径漏洞、IBM WebSphere Application Server 未明跨站脚本漏洞、IBM WebSphere Application Server JAX-WS 拒绝服务漏洞、IBM Systems Director Agent "reset_diragent_keys"不安全文件权限漏洞。攻击者可以利用上述漏洞实施拒绝服务、执行任意代码、提升权限等攻击。其中 IBM OmniFind 相关产品漏洞的安全等级为“高危”。目

前 IBM 已发布了升级补丁修复这些安全漏洞，CNVD 建议用户及时下载更新，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-2010-02966>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02953>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02940>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02937>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02917>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02912>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02909>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02908>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02907>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02906>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02905>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02904>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02903>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02893>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02892>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02884>

2、WebKit 存在多个安全漏洞

WebKit 是一款开源的浏览器引擎。本周，WebKit出现了多个安全漏洞，攻击者利用这些漏洞可以实施拒绝服务、执行任意代码等攻击。CNVD收录的该产品的漏洞包括：WebKit SVG文档中颜色处理远程代码执行漏洞、WebKit字符串整数溢出远程代码执行漏洞、WebKit不充分的随机数生成器漏洞、WebKit 'History'对象同源验证绕过漏洞、WebKit HTML 'Link' DNS预取安全绕过漏洞、WebKit编辑命令远程代码执行漏洞、WebKit WebSockets整数溢出远程代码执行漏洞、WebKit内联样式命令远程代码执行漏洞、WebKit元素属性释放后使用远程代码执行漏洞、WebKit可编辑元素远程代码执行漏洞、WebKit 'Text'对象整数溢出远程代码执行漏洞、WebKit CSS远程代码执行漏洞、WebKit CSS计数器样式远程代码执行漏洞、WebKit CSS框远程代码执行漏洞、WebKit滚动栏释放后使用远程代码执行漏洞、WebKit内联文本框远程代码执行漏洞、WebKit Geolocation对象释放后使用远程代码执行漏洞、WebKit CSS 3D变形远程代码执行漏洞、WebKit SVG文档释放后使用远程代码执行漏洞。目前Webkit的发布厂商Apple已经发布了上述漏洞的补丁更新程序，CNVD提醒广大用户下载更新，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-2010-02988>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02987>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02986>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02985>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02984>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02983>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02982>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02981>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02980>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02979>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02978>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02977>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02976>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02973>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02972>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02971>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02970>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02969>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02967>

3、Cisco Unified Videoconferencing 存在多个安全漏洞

Cisco Unified Videoconferencing 是思科统一通信系统的一个重要组件。CNVD 本周收录的 Cisco Unified Videoconferencing 漏洞包括: Cisco Unified Videoconferencing 弱密码算法漏洞、Cisco Unified Videoconferencing WEB 接口弱会话 COOKIE 会话劫持漏洞、Cisco Unified Videoconferencing shadow 密码可读漏洞、Cisco Unified Videoconferencing 硬编码用户凭据安全绕过漏洞、Cisco Unified Videoconferencing 远程命令注入漏洞、Cisco Unified Videoconferencing FTP 服务器安全漏洞、Cisco Unified Videoconferencing 锁定 OpenSSH 配置漏洞。攻击者可以利用这些漏洞获取敏感信息或提高权限。上述漏洞的安全等级全部为“高危”。目前厂商还未提供详细的解决方案, CNVD 提醒广大用户密切关注厂商主页发布的更新信息并及时下载, 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-2010-02931>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02930>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02925>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02923>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02915>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02914>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02913>

4、Apple Mac OS X 存在多个安全漏洞

Apple Mac OS X 是Mac机器上安装的操作系统。CNVD本周收录的该产品的漏洞包括: Apple Mac OS X Type Services整数错误漏洞、Apple Mac OS X Networking输入验证漏洞、Apple Mac OS X Image Capture输入验证漏洞、Apple Mac OS X ImageIO输入验证漏洞、Apple Mac OS X Image RAW堆缓冲区溢出漏洞、Apple Mac OS X资源管理错误漏洞、Apple Mac OS X Type Services栈缓冲区溢出漏洞、Apple Mac OS X Time Machine设计错误漏洞、Apple Mac OS X OpenSSL加密问题漏洞、Apple Mac OS X Dovecot内存混叠漏洞。攻击者可以利用这些漏洞进行拒绝服务攻击、执行任意代码、获取敏感信息等。目前Apple已发布

了这些漏洞的升级补丁，CNVD建议广大Apple用户及时下载更新，避免相关漏洞引发的安全威胁。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02954>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02952>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02951>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02949>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02945>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02943>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02928>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02927>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02924>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02896>

5、Camtron CMNC-200 出现多个安全漏洞

Camtron CMNC-200 是一款网络摄像机。本周，配套 Camtron CMNC-200 的应用软件出现了 4 个“高危”的漏洞，远程攻击者可能利用这些漏洞可以绕过安全限制、获得敏感信息、实施拒绝服务或任意代码执行等攻击。CNVD 收录的相关漏洞包括：Camtron CMNC-200 权限许可和访问控制漏洞、Camtron CMNC-200 授权问题漏洞、Camtron CMNC-200 管理界面目录遍历漏洞、Camtron CMNC-200 ActiveX 控件缓冲区溢出漏洞。目前部分漏洞已被利用，相关厂商尚未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-2010-02957>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02958>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02959>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02960>

6、Mozilla Firefox跨站脚本攻击漏洞

Mozilla Firefox 是一款非常流行的开放源码的WEB浏览器。本周，Mozilla Firefox出现了一个跨站脚本攻击漏洞。Mozilla Firefox 3.6 Beta 3之前的版本因为不能正确处理超长 UTF-8编码，远程攻击者可以借助特制字符串绕过跨站脚本攻击的保护机制，实施跨站脚本攻击。目前，厂商已经发布了该漏洞的补丁程序，CNVD提醒广大用户及时下载更新，避免引发此漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02934>

小结：本周，Mozilla Firefox、WebKit、Apple Mac OS X、Cisco Unified Videoconferencing、Linux、IBM 的 OmniFind、WebSphere MQ 以及 Systems Director 等多个厂商的多款产品均出现了可被利用的安全漏洞，这些漏洞对用户的信息安全和网络安全构成了较为严重的威胁。请使用上述软件的广大用户注意采取安全防范措施，尽快下载相关补丁程序修复漏洞，做好安全加固工作。



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、Linux 发布安全公告修补了多个漏洞

Linux 是一款开放源代码的操作系统。本周，CNVD 收录了 Linux 相关产品的多个安全漏洞，攻击者可以利用这些漏洞实施拒绝服务攻击。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/1764>

<http://www.cnvd.org.cn/patch/1770>

<http://www.cnvd.org.cn/patch/1748>

<http://www.cnvd.org.cn/patch/1749>



本周要闻速递

1、OpenSSL 更新以修复远程执行漏洞

开源的 SSL 和 TLS 的应用程序的维护者 11 月 16 日警告称，已经在 OpenSSL TLS 中发现一个服务器扩展缓冲区溢出漏洞，受影响的版本包括 OpenSSL 0.9.8o、1.0.0 和 1.0.0a，Apache HTTP 服务器和安全通道则不会受到影响。Red Hat 安全反应小组也警告 Linux 用户称该漏洞可能被远程应用，特定条件下会为远程攻击者触发执行应用程序的权限。目前 OpenSSL 的服务器端程序已经更新，以修复可能造成恶意执行甚至远程安装恶意软件的潜在漏洞。

参考链接：http://tech.ifeng.com/internet/detail_2010_11/17/3136272_0.shtml

2、谷歌 Gmail 等产品曝出安全漏洞

据报道，包括 Gmail 在内的多款谷歌产品日前曝出安全漏洞，可导致用户电子邮箱地址等个人信息泄露。该消息曝光后，谷歌迅速解决了该问题。谷歌在一份声明中称：“该问题存在于 Google Apps 脚本 API (应用编程接口) 中，如果用户访问过特定网站，那么第三方可以在未经用户许可前提下向用户发送电子邮件。如今，我们已经迅速修复该问题，阻止了存在问题的网站。我们希望大家负责任地公开产品的安全问题，并发送到 security@google.com。”

参考链接：<http://tech.sina.com.cn/i/2010-11-21/10154890413.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