

信息安全漏洞周报

2010年9月06日-2010年9月12日

2010年第35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 130 个，其中高危漏洞 24 个、中危漏洞 49 个、低危漏洞 57 个。上述漏洞中，可利用来实施远程攻击的漏洞有 113 个。经跟踪发现，网上已经出现针对 Adobe Reader 和 Acrobat 字体解析缓冲区溢出漏洞、Adobe 多款应用程序的“非信任搜索路径漏洞”、“Windows Program Group 非信任搜索路径漏洞”和“Cisco Packet Tracer 非信任搜索路径漏洞”的零日攻击代码，请上述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 62 个漏洞由相关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、Adobe Reader 和 Acrobat 存在字体解析缓冲区溢出漏洞

运行于 Mac OS、Windows、UNIX 上的 Adobe Reader 9.3.4 及之前版本、运行于 Windows 和 Mac OS 上的 Adobe Acrobat 9.3.4 及之前版本均存在字体解析缓冲区溢出漏洞。攻击者利用漏洞可导致系统崩溃或获取系统控制权限。目前此漏洞正在被恶意攻击者广泛利用。Adobe 已发布安全公告（APSA10-02）并表示正在开发相应的漏洞补丁，建议用户先使用微软的 EMET 2.0(增强减灾体验工具)来避免受到此漏洞的影响，并继续关注 Adobe 官网，以便及时下载补丁更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01926>

2、Google Chrome 存在多个安全漏洞

Google Chrome 是一款开源的 WEB 浏览器。Google Chrome 存在多个安全漏洞，攻击者可利用漏洞实施拒绝服务、跨域脚本、绕过安全限制、执行任意代码等攻击。具体漏洞包括：利用空帧目标绕过弹出式窗口拦截器保护的漏洞、利用单应性序列进行 URL 地址栏视觉欺骗漏洞、存在可绕过限制访问剪贴板内容的漏洞、SVG 过滤器使用失效指针漏洞、存在可枚举安装的扩展漏洞、WebSockets 存在空指针应用浏览器崩溃漏洞、Notifications

presenter存在释放后使用漏洞、权限通告存在内存破坏漏洞、websocket存在整数错误漏洞、计数器节点存在内存破坏漏洞、存在存储大量自动完成项的漏洞、处理focus事件时存在内存破坏漏洞、沙盒参数存在反序列化漏洞、存在跨域图像窃取漏洞。目前Google Chrome 6.0.472.53版本已修复上述安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01923>

3、Mozilla Firefox/Thunderbird/SeaMonkey 存在多个安全漏洞

Mozilla Firefox/Thunderbird/SeaMonkey 是 Mozilla 发布的 WEB 浏览器/邮件/新闻组客户端程序。Mozilla Firefox/Thunderbird/SeaMonkey 存在多个安全漏洞，远程攻击者可利用漏洞获得敏感信息、绕过安全限制或以应用程序权限执行任意代码。具体漏洞包括：浏览器引擎存在未明漏洞、框架元素实现存在整数溢出漏洞、“navigator.plugins”的实现存在漏洞、在转换文本运行时存在漏洞、处理 XUL 树选定存在释放后使用的漏洞、“nsTreeContentView”存在漏洞、在规格化文档时存在漏洞、处理应用于文档中的字体时存在漏洞、“XPCSafeJSObjectWrapper” (SJOW)封装类存在逻辑漏洞、文档拷贝粘贴和拖放 HTML 代码时存在漏洞、跨源提交存在漏洞、处理<object>标签的类型属性时存在漏洞。目前 Mozilla 已发布更新程序以修复上述漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01973>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01976>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01978>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01980>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01981>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01985>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01986>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01987>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01988>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01990>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01991>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01992>

4、Cisco Wireless LAN Controller存在多个安全漏洞

Cisco Wireless LAN Controller是使用轻量级接入点协议(LWAPP)管理Cisco Aironet接入点的应用设备。Cisco Wireless LAN Controller存在多个安全漏洞，远程攻击者可利用漏洞执行拒绝服务攻击或读权限修改设备配置。具体漏洞包括：Cisco Wireless LAN Controller ACL安全绕过漏洞、Cisco Wireless LAN Controller IKE报文处理拒绝服务漏洞、Cisco Wireless LAN Controller HTTP报文拒绝服务漏洞、Cisco Wireless LAN Controller远程特权提升漏洞。目前Cisco已经发布安全公告（cisco-sa-20100908-wlc）及补丁修复上述安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01938>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01943>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01944>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01945>

5、Linux 内核存在多个安全漏洞

Linux Kernel是开放源操作系统Linux所使用的内核程序。Linux内核存在多个安全漏洞，攻击者可利用这些漏洞执行拒绝服务攻击。具体漏洞包括：Linux Kernel fs/cifs/cifssmb.c文件输入验证漏洞、Linux kernel ‘net/irda/af_irda.c’ 中irda_bind（）函数资源管理错误漏洞、Linux kernel ‘mm/memory.c’ 中do_anonymous_page（）函数代码注入漏洞、Linux内核“xfs_ioc_fsgetxattr()”内存泄漏漏洞、Linux内核‘snd_seq_oss_open()’本地内存破坏漏洞、Linux Kernel “niu_get_ethtool_tcam_all()”缓冲区溢出漏洞、Linux Kernel JFS xattr命名控件访问规则安全绕过漏洞、Linux Kernel GFS2目录重命名空指针应用本地拒绝服务漏洞。目前厂商已经发布升级补丁修复上述安全漏洞，建议相关用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01954>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01961>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01962>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01963>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01949>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01950>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01982>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01907>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01922>

小结：本周，Adobe 公司发布公告称 Adobe Reader 和 Acrobat 软件中存在高危“零日”字体解析缓冲区溢出漏洞，并已被攻击者利用。此外，Chrome、Firefox、Linux Kernel 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、Apple 发布更新程序

Apple IOS 是一款运行在苹果 iPhone 和 iPod touch 设备上的操作系统。Apple 发布更新程序 Apple IOS 4.1 以修复 Apple IOS 中存在的多个安全漏洞，这些漏洞包括：Apple IOS 在 WebKit 处理选择器的时候存在两次释放漏洞、Apple IOS 在 WebKit 处理 SVG 文档中的“use”元素时存在内存损坏漏洞、Apple IOS 存在通过特殊构建的 TIFF 图像可导致破坏内存并执行任意代码漏洞、Apple IOS 在渲染内联元素时诱使用户访问破坏内存或执行任意代码漏洞等。CNVD 提醒广大用户为避免遭受漏洞影响请及时下载补丁更新。

补丁下载链接：<http://www.cnvd.org.cn/patch/977>

<http://www.cnvd.org.cn/patch/978>

<http://www.cnvd.org.cn/patch/979>

<http://www.cnvd.org.cn/patch/981>

本周要闻速递

1、Adobe 曝出最新高危漏洞

9月10日，Adobe公司发公告称，AdobeReader、Acrobat软件中均存在一个高危“零日”漏洞，并已被攻击者利用。Adobe在安全公告中指出，微软Windows、苹果Mac以及Unix平台上的AdobeReader9.3.4及更早版本、Windows、Mac平台上的Acrobat9.3.4及更早版本中均受此漏洞影响，这个漏洞（CVE-2010-2883）会导致系统崩溃，黑客可能会利用该漏洞完全控制计算机，并令这种危险扩散到数以百万计的受害者。目前Adobe方面正在开发相应的漏洞补丁，建议用户先使用微软的EMET 2.0(增强减灾体验工具)来避免受到此漏洞的影响。

参考链接：<http://it.people.com.cn/GB/42891/42898/12710456.html>

<http://it.chinabyte.com/54/11537554.shtml>

2、微软下周二将发布9个补丁修复13个安全漏洞

9月9日，微软表示下周二将发布9个安全补丁，修复13个安全漏洞。这些安全漏洞影响到Windows、互联网信息服务和微软Office等软件。据微软安全反应中心的博客称，有4个补丁是“严重”等级的，其余的是“重要”等级的。受影响的软件包括Windows XP、Vista和Windows 7；Windows Server 2003和2008；Office XP、2003和2007。需要注意的是，Windows XP SP2已经得不到任何官方补丁修复，建议使用SP2的用户尽快升级到SP3。此外，之前爆出的可以影响数百个应用程序安全的Windows DLL漏洞也有可能将在本次安全更新中得以修复。

参考链接：<http://sec.chinabyte.com/140/11537140.shtml>

<http://pcedu.pconline.com.cn/softnews/gdpl/1009/2217892.html>

3、IOS4.1再现越狱漏洞，涉及产品iPad和Touch

在苹果公司于9月9日发布IOS 4.1智能操作系统更新之后，IOS 4.1又被发现存在越狱漏洞。所谓的越狱就是将苹果设备系统进行破解，从而让其可以支持那些未经苹果公司官方认证的第三方应用程序。据iPhone Dev Team越狱团队透露，本次基于启动ROM的最新越狱漏洞需要用到一个硬件方面的重要改变，而苹果方面做出这一改变的初衷居然就是为了封堵之前出现的越狱漏洞。另外新的IOS 4.1越狱不但可以在iPhone 4智能手机上适用，同时也可以用在iPad平板和第四代iPod Touch播放器上适用。

参考链接：<http://tech.163.com/mobile/10/0910/06/6G6V4EMN00112K8E.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