

信息安全漏洞周报

2010年9月20日-2010年9月26日

2010年第37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 84 个,其中高危漏洞 2 个、中危漏洞 30 个、低危漏洞 52 个。上述漏洞中,可利用来实施远程攻击的漏洞有 72 个,0day 漏洞 6 个,CNVD 提醒广大互联网用户提高警惕,加强防范措施。本周收录的安全漏洞中,已有 58 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、Cisco 多款产品存在安全漏洞

Cisco公司的IOS H.323 packets、IOS H.323 traffic、Unified Communications Manager、IOS SSL VPN、IOS SIP、IOS NAT、IOS IGMPv3等产品及组件存在多个安全漏洞,攻击者可利用这些漏洞执行拒绝服务攻击。具体漏洞包括: Cisco IOS H.323 packets存在拒绝服务漏洞、Cisco IOS H.323 traffic存在拒绝服务漏洞、Cisco Unified Communications Manager使用UDP协议时SIP注册实现存在错误漏洞、Cisco Unified Communications Manager处理非法"Refer-To"头时存在错误漏洞、Cisco IOS SSL VPN存在拒绝服务漏洞、Cisco IOS SIP packets存在拒绝服务漏洞、Cisco IOS SIP traffic 存在拒绝服务漏洞、Cisco IOS SIP 消息处理存在拒绝服务漏洞、Cisco IOS NAT for H.225.0存在拒绝服务漏洞、Cisco IOS NAT for H.323存在拒绝服务漏洞、Cisco IOS NAT FOR SIP存在拒绝服务漏洞、Cisco IOS IGMPv3存在两个拒绝服务漏洞。目前Cisco已经发布安全公告及补丁修复上述安全漏洞,建议相关用户尽快下载更新。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-02136>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02135>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02133>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02134>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02139>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02138>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02137>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02144>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02140>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02141>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02142>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02143>

2、IBM 多款产品存在安全漏洞

IBM 的 FileNet P8 Application Engine Workplace、FileNet P8 Application Engine Image Viewer、WebSphere Application Server 等产品和组件存在多个安全漏洞，攻击者可利用这些漏洞获得非授权敏感信息，用于提升权限，并可以利用漏洞执行跨站脚本、拒绝服务、网页仿冒和劫持 Web 会话等攻击。具体漏洞包括：IBM FileNet P8 Application Engine Workplace 组件权限许可和访问控制漏洞（CVE-2009-5001、CVE-2009-4998）、IBM FileNet P8 Application Engine Workplace 组件信任管理和敏感信息泄露漏洞、IBM FileNet P8 Application Engine Workplace 组件未明权限许可和访问控制漏洞、IBM FileNet P8 Application Engine Image Viewer 组件权限许可和访问控制漏洞、IBM FileNet P8 Application Engine Workplace 组件跨站脚本攻击漏洞、IBM FileNet P8 Application Engine Workplace 组件多个跨站脚本攻击漏洞、IBM FileNet Application Engine Workplace 组件安全绕过漏洞、IBM FileNet Application Engine Workplace 组件跨站脚本攻击漏洞(CVE-2010-3470)、IBM FileNet Application Engine Workplace 会话固定漏洞、IBM FileNet Application Engine Workplace 组件多个跨站脚本攻击漏洞(CVE-2010-3472)、IBM FileNet Application Engine Workplace 组件开放重定向漏洞、IBM WebSphere Application Server 管理控制台存在拒绝服务漏洞。目前，上述漏洞均有解决方案，建议相关用户参照及时采取加固措施。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02202>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02200>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02198>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02183>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02206>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02205>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02204>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02203>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02187>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02186>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02185>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02184>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02152>

3、Linux Kernel内核及Linux-PAM模块存在多个安全漏洞

Linux是一款开放源代码的操作系统。Linux Kernel内核及Linux-PAM模块出现了多个安全漏洞，攻击者可利用漏洞获取普通用户和管理员权限，进而发动破坏内存、泄漏信息、拒绝服务等网络攻击。具体漏洞包含：Linux Kernel DE4X5_GET_REG请求内核信息泄露漏洞、Linux Kernel “sctp_outq_flush（）”函数拒绝服务漏洞、Linux-PAM “pam_env”和“pam_mail”模块存在安全漏洞、Linux-PAM “pam_env”和“pam_mail”模块setfsuid()函数访问验证漏洞、Linux Kernel “rose_bind（）”函数和“rose_connect（）”函数内存破坏漏洞、Linux Kernel Ptrace（CVE-2010-3301）本地特权提升漏洞。目前，上述漏洞均有解决方案，建议相关用户参照及时采取加固措施。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02130>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02179>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02178>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02161>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02160>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02157>

4、Google浏览器Chrome存在两个高危漏洞

谷歌浏览器Chrome存在两个高危漏洞。一个是Google Chrome缓冲区溢出漏洞，Google Chrome 6.0.472.59之前版本在执行地理定位功能时，不能在Google地图上准确定位，远程攻击者可以借助未知向量发起拒绝服务或其它网络攻击；另一个是Google Chrome 文件对话框拒绝服务漏洞，基于Mac OS X平台的Google Chrome 6.0.472.59之前版本不能正确执行文件对话框，远程攻击者可以借助未知向量发动拒绝服务或其它网络攻击。Google已经发布公告及更新程序修复上述安全漏洞，建议相关用户尽快下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02201>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02190>

小结：本周，思科产品出现了12个漏洞，对众多采用其网络设备及应用软件的企事业单位构成较为严重的安全威胁，应及时采取修补措施；另外IBM多个产品、Linux Kernel内核及Linux-PAM模块、Google Chrome等均出现安全漏洞，这些漏洞对相关用户的信息安全和网络安全均构成威胁，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、Firefox js_InitRandom函数的安全补丁公告

Firefox是一款非常流行的开源WEB浏览器。Firefox的JavaScript实现中的js_InitRandom函数使用了当前时间或环境相关的指针作为随机数生成器的种子，攻击者可以通过暴力猜解攻击相对容易地获得种子值，从而执行劫持会话等各种攻击。Firefox已发

布的补丁程序修补了漏洞。CNVD 提醒广大用户尽快下载安装补丁程序，避免引发漏洞相关的网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patch/1110>

本周要闻速递

1、Twitter 称安全漏洞已被修复

9 月 22 日消息，根据 Twitter 安全主管的说法，先前爆出的 Twitter 安全漏洞已被“完全修复”。Twitter 爆出的安全漏洞涉及 onMouseOver JavaScript 编码，导致用户在不知情的情况下，被定向至第三方网站。众多用户中招，受害者包括英国前首相布朗的妻子莎拉·布朗。运营 4 年的 Twitter 用户数已经超过 1.45 亿，现平均每天增加 37 万新用户。

要闻参考链接：<http://it.sohu.com/20100922/n275203955.shtml>

2、半数企业应用软件存在漏洞

应用程序安全公司 Veracode 近日发布的一份研究报告显示，企业中使用软件，超过一半存在安全问题。Veracode 最近 18 个月以来分析了来自于使用云服务的用户超过 2900 个应用程序，发现这些软件中有 57% 存在不可预知的安全问题。报告显示，企业日常使用中的第三方代码往往是不安全的，81% 的第三方应用程序供应商未能达到可接受的安全标准。Veracode 还表示，跨站脚本漏洞是最常见的应用程序漏洞，.Net 应用程序有着超乎平常的安全缺陷率。同日 WhiteHat Security 也发表了一份报告显示，平均每个网站有将近 13 个严重安全漏洞。

要闻参考链接：http://security.zdnet.com.cn/security_zone/2010/0926/1898094.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