

信息安全漏洞周报

2010年5月3日-2010年5月9日

2010年第18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)本周共收集和整理信息安全漏洞 36 个,其中高危漏洞 6 个、中危漏洞 6 个、低危漏洞 24 个。上述漏洞中,可利用来实施远程攻击的漏洞有 30 个。经检测发现,网上已经出现针对“IBM WebSphere Application Server SIP 日志信息泄漏漏洞”的零日攻击代码,请广大用户注意做好防护措施。目前,相关厂商已经为 24 个漏洞提供了修补方案,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、暴风影音播放器 m3u 文件处理远程溢出漏洞

暴风影音是一款国内流行的多媒体播放软件。暴风影音播放器在处理m3u文件时存在边界检查错误,从而导致了溢出漏洞。攻击者可以通过欺骗用户点击特殊构造的m3u播放文件,最终达到控制用户操作系统的目的。目前,暴风影音官网已经发布暴风影音播放器的更新版本3.10.04.29和CNTV_Beta2 3.10.04.27,建议使用该播放器的用户尽快下载升级。
参考链接: <http://www.baofeng.com/>

2、Microsoft Windows 的 SMTP 服务存在两个安全漏洞

Microsoft Windows是微软发布的非常流行的操作系统。Windows的SMTP服务存在两个安全漏洞: Microsoft Windows SMTP服务DNS响应字段验证DNS欺骗漏洞, Windows系统中的SMTP服务没有检查从网络接收到的DNS响应的ID字段值是否与之前所发送的DNS查询报文的ID字段值相匹配, 恶意服务器可以通过返回伪造的查询响应执行中间人等网络欺骗攻击; Microsoft Windows SMTP服务可预测DNS查询ID漏洞, 即Windows系统中的SMTP服务所生成的DNS查询中的transaction ID字段值是可预测的, 恶意服务器可以相对容易的破解随机数, 并通过伪造响应执行中间人等网络欺骗攻击。微软在4月发布的安全公告 (MS10-024) 已经修复了以上安全漏洞, 建议尚未安装补丁的用户尽快下载使用。

参考链接: <http://www.microsoft.com/technet/security/bulletin/MS10-024.msp?pf=true>

3、Microsoft Visio VISIODWG.DLL库缓冲区溢出漏洞

Visio是MSOffice套件中的图形编辑工具。Visio中所使用的VISIODWG.DLL库中存在缓冲区溢出漏洞，起因是在该库的74ef偏移处执行了不安全的strcpy调用。在将DXF文件注入到Visio文档中时（通过拖放操作或从菜单栏中选择“注入 -> CAD绘图”）会加载有漏洞的函数库。成功利用这个漏洞的攻击者可以以Visio用户权限执行任意代码。微软在4月发布的安全公告（MS10-028）已经修复了以上安全漏洞，建议尚未安装补丁的用户尽快下载使用。

参考链接：<http://www.microsoft.com/technet/security/bulletin/MS10-028.msp?pf=true>

4、IBM Websphere 应用服务器存在两个高危安全漏洞

IBM Websphere应用服务器以Java和Servlet引擎为基础，支持多种HTTP服务，可帮助用户完成从开发、部署到维护交互式动态网站的所有工作。IBM Websphere应用服务器存在两个高危安全漏洞：IBM WebSphere Application Server -trace选项信息泄露漏洞，在启用了-trace选项（也称为调试模式）的情况下，WebSphere应用服务器所执行的调试语句会打印出某些对象的字符串表示，本地用户可以通过读取、追踪上述输出获得敏感信息；IBM WebSphere Application Server SIP日志信息泄漏漏洞，在启用了完整SIP跟踪日志的配置下，服务器接收或发送SIP消息时，会把整个SIP消息写到跟踪文件中，包括所有头字段和消息体信息，其中还可能包括敏感信息。目前厂商已经发布了升级补丁以修复这个安全问题，建议用户尽快下载使用。

参考链接：<http://www.ibm.com/support/docview.wss?rs=180&uid=swg27004980>

5、OpenTTD 存在多个安全漏洞

OpenTTD是一款Microprose发行的运输大亨豪华版(TTD) 游戏的开源版。OpenTTD存在多个安全漏洞，恶意用户可利用漏洞进行拒绝服务攻击。具体漏洞信息为：OpenTTD密码请求处理远程拒绝服务漏洞、OpenTTD地图不完全下载消耗文件描述符导致远程拒绝服务漏洞、OpenTTD远程代码执行漏洞。目前，OpenTTD 1.0.1已经修复了该漏洞，建议用户尽快下载使用。

参考链接：<http://www.openttd.org/>

小结：本周 CNVD 所整理的漏洞信息中，暴风影音播放器、Windows 的 SMTP 服务、Visio 编辑工具、IBM Websphere 应用服务器等流行软件均出现了严重漏洞。危害我国网民的用网安全，请广大用户注意采取安全防范措施，尽快下载相关补丁程序。



本周重要漏洞修补信息

本周，CNVD 整理和发布以下重要漏洞修补信息。

1、Red Hat Bugzilla 安全公告

Red Hat Bugzilla 于 5 月 7 日发布了安全公告(Bug 572971)以及相应补丁,修复了 Red Hat Xen MMIO 指令解码器本地客户机拒绝服务漏洞。建议用户尽快下载使用,避免本地攻击者利用漏洞使应用程序崩溃。

补丁下载链接: https://bugzilla.redhat.com/show_bug.cgi?id=572971



本周要闻速递

1、思科 Wi-Fi 产品被曝存在安全漏洞

据国外媒体报道,德国测试公司 ERNW 的两位研究人员表示思科 Wi-Fi 产品中存在广泛的安全漏洞。他们透露,通过利用共享接入点信息的思科协议中的安全漏洞,有可能实施拒绝服务攻击和嗅探思科结构化无线感知型网络中的加密通讯。同时,这些研究人员在黑客会议上还展示了通过思科统一无线网络设备的管理网页接口对这种设备实施的攻击。实际上,思科的接入点近来已经出现几次安全隐患。此前思科无线 LAN 控制器中就被发现过存在安全漏洞,甚至可能导致攻击者向 Wi-Fi 网络发送恶意信息。思科部分产品中 Aironet Wi-Fi 接点也曾经有过缺陷,这些缺陷可能会被黑客利用。这些有缺陷的接入点用未加密文本形式实行无线传送安全密钥,这意味着黑客可以在中途截取。有了这些密钥,黑客能轻而易举地破坏加密的 Wi-Fi 传输。

参考链接: <http://www.hackbase.com/news/2010-05-08/35124.html>

2、飓风木马暴力劫持搜索引擎

近日,大量网民受到了一款“飓风木马”的侵害,网民的浏览器首页被篡改改为 www.91kk.com 或者是 123.sogou.com。据安全专家介绍,“飓风木马”却是一款极具破坏力的恶性木马,它通过劫持中招用户的网络来保护自己,阻止多数主流安全软件的联网升级。而一旦该木马文件被杀毒软件或用户手工删除后,还会造成电脑断网,普通用户很难自行修复。

参考链接: http://tech.ccidnet.com/art/1102/20100506/2052655_1.html

3、安全公司披露微软上月悄悄修复三个严重漏洞

5 月 7 日消息,据国外媒体报道,一位安全专家本周四称,微软上个月悄悄地修复了三个安全漏洞,其中有两个安全漏洞影响到企业执行重要任务的 Exchange 邮件服务器。据 Core 安全技术公司首席技术官说,微软修复了这些安全漏洞,但是,没有披露它修复了这些安全漏洞的消息。这些安全漏洞比微软披露的安全漏洞更加严重。这意味着系统管理员也许会对使用补丁的决策做出错误的决定,他们需要这个信息来评估这个风险。微软承认它在没有告诉用户的情况下修复了一些安全漏洞,并为这种做法进行了辩护。

参考链接: <http://sec.chinabyte.com/100/11305600.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