

信息安全漏洞周报

2010年6月28日-2010年7月4日

2010年第25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 40 个,其中高危漏洞 4 个、中危漏洞 10 个、低危漏洞 26 个。上述漏洞中,可利用来实施远程攻击的漏洞有 38 个。经检测发现,网上已经出现针对“D-Link DAP-1160 无线访问接入点 DCC 协议安全绕过漏洞”和“MySQL ALTER DATABASE 远程拒绝服务漏洞”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 16 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、MySQL "ALTER DATABASE"拒绝服务漏洞

MySQL是一款流行的数据库软件。MySQL在处理"ALTER DATABASE"声明语句时存在漏洞,攻击者可以通过在"#mysql50#"前缀之后附加"."或"..",破坏MySQL的数据目录。MySQL 5.1.48已经修复了该漏洞,建议用户尽快下载更新,避免攻击者利用该漏洞破坏数据库。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-01257>

2、Adobe Flash Player AVM Bytecode多个整数溢出漏洞

Flash Player是一款非常流行的FLASH播放器。Flash Player在解析Adobe的AVM 2 bytecode中的opcode时存在整数溢出漏洞。这个opcode的运算符用作了到结构的偏移,如果设置为恶意的值就可能执行攻击者预设的代码。结构中包含有之后会被调用的函数指针,如果攻击者将受控数据修改为指向无效的偏移,这个函数指针就可能设置为指向恶意的代码,导致以当前运行浏览器用户的权限执行任意代码。此外AVM bytecode验证符中也存在整数溢出漏洞。具体来讲,newFrameState方式在计算栈帧的大小时错误地信任了从bytecode所获得的max_scope和max_stack变量。通过伪造特定的值,就可以溢出表示帧大小的整数,导致以当前运行浏览器用户的权

限执行任意代码。目前厂商已发布了安全公告及相关补丁，建议用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01252>

3、libpng内存破坏和拒绝服务漏洞

libpng是多种应用程序所使用的解析PNG图形格式的函数库。libpng在处理图形行数据时存在缓冲区溢出漏洞，如果图形文件中提供了比头中报告的高度多出一个额外的图形行的话，就会触发缓冲区溢出，导致攻击者在受影响系统上执行任意代码；此外在处理某些sCAL块时可能出现内存泄露，解析特制的PNG图形可能导致拒绝服务。目前libpng 1.2.44和libpng 1.4.3已经修复了上述漏洞，建议用户尽快下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01238>

4、MemDB 多款产品存在远程拒绝服务漏洞

MemDB公司开发内存数据库系统、在线调查系统等软件产品。目前，该公司多款产品存在漏洞，允许攻击者破坏目标系统。在这些产品的应用过程中，当解析HTTP "Host"头字段数据时，嵌入式WEB服务器存在边界错误，可触发基于栈的缓冲区溢出。目前厂商尚未发布补丁或更新程序，建议用户继续关注厂商主页以获得解决方案。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-01256>

小结：本周CNVD收集的漏洞信息中，MySQL、Adobe Flash Player、libpng等应用广泛的软件出现高危漏洞，可被攻击者利用来执行恶意代码或实施拒绝服务攻击，对国内网民的上网安全构成严重威胁。请使用上述软件的用户注意采取安全防范措施。

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、Opera Web 浏览器 10.60 更新修复多个安全漏洞

Opera Software 发布了 Opera Web Browser 安全公告及相关补丁信息，修复了Opera10.60 之前版本中存在的多个安全漏洞。建议用户尽快下载补丁程序修复漏洞，避免远程攻击者利用漏洞获得敏感信息或以应用程序权限执行任意命令。

补丁下载链接：<http://www.cnvd.org.cn/patch/562>



本周要闻速递

1、谷歌承认 Youtube 网站遭到黑客攻击

恶意黑客星期日利用谷歌 Youtube 网站上的跨站脚本安全漏洞对这个非常流行的视频共享网站实施了攻击。这次攻击主要影响到 Youtube 网站用户发表评论的栏目。据熟悉这种攻击的业内人士称,虽然这种攻击本身没有包含恶意感染,但是,这种风险是当用户访问任何这种被攻击的网页时,攻击者会把用户引导到其它网站。目前还不清楚 Youtube 网站的登录页是否包含恶意软件,但是,最新的杀毒软件可以防御这种威胁。

参考链接: <http://www.cnbeta.com/articles/115470.htm>

2、一种针对 MSN 和 Windows Live 的新威胁已出现

根据安全厂商 G Data 的警告,一种针对 MSN Messenger 和 Windows Live Messenger 的新威胁已经出现。该公司研究发现连接到这两个服务的垃圾邮件和钓鱼网站呈爆发趋势,并且大多以虚假的好友请求出现。安全厂商 Trusteer 说他们已经掌握了一种恶意软件攻击,它可以通过创造虚假的银行登录页面来窃取用户的账号进行转账。该公司提醒英国的银行用户注意这种威胁,它可以通过网站和垃圾邮件中的附件进行传播。与此同时,赛门铁克公司也发现了一种针对国防承包商的攻击,方式包括黑掉某承包商公司网站来向另一承包商发动恶意软件攻击。这种攻击的灵巧性和复杂性特别值得关注。

参考链接: <http://www.hackbase.com/news/2010-07-04/36243.html>

3、利用 Windows 帮助 Oday 漏洞的恶意软件迅速增加

微软周三表示,其安全团队已检测到超过 10,000 个攻击 Windows 帮助和支持中心 Oday 漏洞的案例,该漏洞早在 6 月 10 日被研究人员披露,可影响 Windows XP 和 Server 2003 计算机并安装恶意软件。漏洞公布 10 天以来袭击目标相对较少,而在过去的一周半时间里,微软恶意软件保护中心发现来自美国,俄罗斯,葡萄牙,德国和巴西的攻击数量大大上升。新增的攻击大多用来被下载恶意软件知名的后门,包括 Win32/Swrort.A, Win32/Tedroo.AB, Win32/Oficla.M 和 Win32/Neetro.A 等品种。微软呼吁用户在打补丁的同时部署额外的安全方法,让这一安全漏洞的影响减到最小。

参考链接: <http://www.hackbase.com/news/2010-07-01/36190.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