

信息安全漏洞周报（双周并刊）

2010年9月27日-2010年10月10日

2010年第38-39期

双周漏洞基本情况

9月27日至10月10日，信息安全漏洞威胁整体评价级别为**中**。

期间，国家信息安全漏洞共享平台（以下简称CNVD）共收集和整理信息安全漏洞104个，其中高危漏洞23个、中危漏洞5个、低危漏洞76个。上述漏洞中，可利用来实施远程攻击的漏洞有83个，0day漏洞14个，CNVD提醒广大互联网用户提高警惕，加强防范措施。其中84个漏洞已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，避免因漏洞引发的网络信息安全事件。

双周重要漏洞信息

9月27日至10月10日，CNVD整理和发布以下重要安全漏洞信息。

1、IBM TSM FastBack 存在多个远程代码执行漏洞

IBM TSM FastBack是一款提供持续数据保护功能和文件服务器恢复技术的套件。IBM TSM FastBack出现了多个安全漏洞，攻击者可以利用漏洞执行任意指令。具体漏洞包括：IBM TSM FastBack加载服务任意覆盖远程代码执行漏洞、IBM TSM FastBack FastBack USER_S_AddADGroup远程代码执行漏洞、IBM TSM FastBack FastBack FXCLI_checkIndexDBLocation远程代码执行漏洞、IBM TSM FastBack FastBack _CalcHashValueWithLength远程拒绝服务漏洞、IBM TSM FastBack Server _Eventlog远程代码执行漏洞、IBM TSM FastBack Server _DAS_ReadBlockReply远程拒绝服务漏洞、IBM TSM FastBack Server ActivateLTScriptReply远程代码执行漏洞、IBM TSM FastBack Server FXCLI_OraBR_Exec_Command远程代码执行漏洞、IBM TSM FastBack Server _SendToLog远程代码执行漏洞。目前IBM已经发布安全公告及补丁修复上述安全漏洞，建议用户尽快下载更新。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02243>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02244>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02245>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02247>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02249>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02250>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02252>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02254>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02256>

2、Linux Kernel 存在多个安全漏洞

开源操作系统 Linux 的内核代码 Linux kernel 存在多个安全漏洞，攻击者可以利用漏洞获得敏感内存信息。具体漏洞包括：Linux Kernel "VIAFB_GET_INFO" IOCTL 信息泄漏漏洞、Linux Kernel FBIOGET_VBLANK "drivers/video/ivtv/ivtvfb.c" 信息泄漏漏洞、Linux Kernel FBIOGET_VBLANK "drivers/video/sis/sis_main.c" 信息泄漏漏洞、Linux Kernel "ipc/sem.c" 信息泄漏漏洞、Linux Kernel TIOCGICOUNT "usb/serial/mos*.c" 信息泄漏漏洞、Linux Kernel TIOCGICOUNT "serial_core.c" 信息泄漏漏洞、Linux Kernel TIOCGICOUNT "drivers/char/nozomi.c" 信息泄漏漏洞、Linux Kernel "SNDRV_HDSP_IOCTL_GET_CONFIG" IOCTL 信息泄漏漏洞。目前，厂商已经发布解决方案，建议用户参照进行安全加固。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02222>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02221>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02220>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02219>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02218>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02217>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02216>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02215>

3、Microsoft Word 2003 存在 MSO 空指针引用漏洞

Microsoft Word 是微软公司开发的一款广泛使用的文字处理系统软件。Microsoft Word MSO.dll 库在处理文件中特殊构建的缓冲区时存在错误，攻击者可利用漏洞进行空指针应用攻击，通过诱使用户解析经特殊构建的恶意 WORD 文件，触发由读取非法内存引起的空指针异常。目前微软公司尚未提供解决方案，请用户随时关注厂商的主页以获取安全加固措施。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02262>

4、GNU Mailman 存在多个跨站脚本漏洞

GNU Mailman 是一款用于管理邮件列表的应用程序。GNU Mailman 存在多个输入验证问题，远程攻击者可以利用漏洞进行跨站脚本攻击，获得敏感信息或劫持目标用户会话。具体漏洞信息包括：Mailman 邮件列表管理器没有正确过滤由通用邮件列表信息提供的邮件列表描述、Mailman 邮件列表管理器在把邮件列表信息内容 HTML 模板渲染给用户之前缺少充分过滤。目前，厂商已经发布解决方案，建议用户参照进行安全加固。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02294>

5、MySQL 存在多个安全漏洞

MySQL 是一款流行的数据库服务软件。MySQL 存在多个安全漏洞，允许恶意用户提升

特权或进行拒绝服务攻击。具体漏洞包括：MySQL "PolyFromWKB()"函数存在漏洞、MySQL处理存储过程中嵌套的Join操作时存在漏洞、MySQL使用中间临时表时处理"GREATEST()"或"LEAST()"函数存在漏洞、MySQL处理与"WITH ROLLUP"组合使用的"GROUP_CONCAT()"时存在漏洞、MySQL重新计算用于临时表的表达式值时存在漏洞、MySQL例化需要临时表的衍生表格时存在漏洞、MySQL处理参数传递给"LEAST()"或"GREATEST()"函数存在漏洞、MySQL处理评注信息时复制操作存在漏洞。目前，厂商已经发布解决方案，建议用户参照进行安全加固。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02224>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02225>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02226>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02227>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02228>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02229>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02230>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02231>

小结： IBM、MYSQL、Linux、Microsoft Word等这些应用广泛的软件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。

双周重要漏洞修补信息

9月27日至10月10日，CNVD整理和发布以下重要安全修补信息。

1、Adobe 发布安全公告修复了 Adobe Reader/Acrobat 的多个漏洞

Adobe 于10月5日发布了安全公告，发布补丁修复了包括 Adobe Acrobat 9.3.4 及之前版本、Adobe Reader 8.2.4 及之前版本的23个高危漏洞，远程攻击者可以利用漏洞获得敏感信息或进行拒绝服务攻击。建议用户尽快下载补丁修复漏洞，以避免遭受漏洞影响。

补丁下载链接：<http://www.cnvd.org.cn/patch/1203>
<http://www.cnvd.org.cn/patch/1204>
<http://www.cnvd.org.cn/patch/1205>
<http://www.cnvd.org.cn/patch/1206>
<http://www.cnvd.org.cn/patch/1207>
<http://www.cnvd.org.cn/patch/1208>
<http://www.cnvd.org.cn/patch/1209>
<http://www.cnvd.org.cn/patch/1210>
<http://www.cnvd.org.cn/patch/1211>
<http://www.cnvd.org.cn/patch/1212>

<http://www.cnvd.org.cn/patch/1213>
<http://www.cnvd.org.cn/patch/1214>
<http://www.cnvd.org.cn/patch/1215>
<http://www.cnvd.org.cn/patch/1216>
<http://www.cnvd.org.cn/patch/1217>
<http://www.cnvd.org.cn/patch/1218>
<http://www.cnvd.org.cn/patch/1219>
<http://www.cnvd.org.cn/patch/1220>
<http://www.cnvd.org.cn/patch/1221>
<http://www.cnvd.org.cn/patch/1222>
<http://www.cnvd.org.cn/patch/1223>
<http://www.cnvd.org.cn/patch/1224>
<http://www.cnvd.org.cn/patch/1225>

双周协调处理的典型事件

协调处理“百度影视跨站漏洞”事件

10月7日，CNVD接到会员单位报送的“百度影视网站跨站漏洞”，CNVD秘书处经过验证核实，及时与百度公司安全技术部门取得联系，并通报了漏洞信息。百度公司也在第一时间将处理意见返回CNVD秘书处。经核实，该漏洞目前已经修复。

双周要闻速递

1、微软发布紧急补丁 修复 ASP.NET 漏洞

微软9月28日发布了一个紧急补丁，修复了之前曝光的存在于ASP.NET中的一个漏洞。该漏洞会导致信息泄露——攻击者能利用这个漏洞查看目标服务器的加密数据、读取目标服务器上的文件数据，攻击者还能利用这个漏洞对服务器进行解密并任意篡改数据内容。微软指出，.NET Framework 3.5 SP1 之前的版本并不受此漏洞影响。微软将此次发布的补丁定级为重要，适用于除了.NET Framework 1.0 SP3 之外的当前所有ASP.NET版本。当前微软仅在下载中心提供了该补丁，微软建议管理员、企业用户和终端用户到下载中心手动下载并安装该补丁。

参考链接：<http://tech.163.com/digi/10/0929/10/6HO8KIHf00162OUT.html>

<http://www.microsoft.com/technet/security/bulletin/ms10-070.mspx>

2、微软将迎来迄今最大补丁日 一次修补 49 个漏洞

据国外媒体报道，微软下周将发布16个补丁程序，总计修复高达49处漏洞，是迄今为止修复漏洞数量最多的一个“补丁日”。在这16个补丁程序中，4个补丁的安全级别为“Critical”，10个为“important”，2个为“moderate”。受上述漏洞影响的产品包括Windows XP、Vista、Windows 7、Windows Server 2003 和 2008、Microsoft Office XP Service Pack 3、Office

2003 Service Pack 3、Office 2007 Service Pack 2、Office 2010、Office 2004 for Mac 、Office 2008 for Mac、Windows SharePoint Services 3.0、SharePoint Server 2007、Groove Server 2010 和 Office Web Apps。

参考链接: <http://tech.sina.com.cn/it/2010-10-10/15314728901.shtml>

3、近七成 iPhone 应用存漏洞 或致信息泄露

据国外媒体报道,近期公布的一项研究报告显示,目前比较流行的 iPhone 手机应用软件中,有近三分之二的应用软件在每次启动时,会伴随发送未加密独立识别码(UDID),而这些数据包含有用户个人信息,部分应用甚至会泄露用户姓名。苹果公司也采取了部分措施,尽量减少 iOS 设备当中所存在的安全隐患。用户使用的应用若是包含有 GPS 或者是通讯地址等个人信息时,程序会自动要求获得用户批准,否则将不允许应用软件正常使用。

参考链接: <http://it.sohu.com/20101005/n275431534.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