

信息安全漏洞周报

2010年10月11日-2010年10月17日

2010年第40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 102 个，其中高危漏洞 15 个、中危漏洞 51 个、低危漏洞 36 个。上述漏洞中，可利用来实施远程攻击的漏洞有 97 个。经跟踪发现，网上已经出现针对“Windows Media Player 远程代码执行漏洞”和“Phpcms 2008 sp4 路径泄露和任意文件删除漏洞”的零日攻击代码，请相关用户注意做好相关防护措施。本周收录的安全漏洞中，已有 95 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，避免遭受侵害。

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、Microsoft 多个应用软件存在安全漏洞

Microsoft的Windows操作系统、IE浏览器、Office办公套件、Microsoft 服务器软件和.Net framework中共存在49处安全漏洞，攻击者可以利用这些漏洞进行拒绝服务、任意代码执行、权限提升、信息泄露、篡改等攻击。具体漏洞包括：Microsoft Windows Failover集群文件权限安全绕过漏洞、Microsoft Windows通用控件链接库远程堆缓冲区溢出漏洞、Microsoft Word书签处理(CVE-2010-3216)远程代码执行漏洞、Microsoft Excel越界内存写(CVE-2010-3241)远程代码执行漏洞、Microsoft Excel记录验证(CVE-2010-3240)远程代码执行漏洞、Microsoft Excel记录验证(CVE-2010-3239)远程代码执行漏洞、Microsoft Excel Negative Future函数(CVE-2010-3238)远程代码执行漏洞、Microsoft Excel合并单元格记录指针(CVE-2010-3237)远程代码执行漏洞、Microsoft Excel越界数组(CVE-2010-3236)远程代码执行漏洞、Microsoft Excel BIFF记录解析(CVE-2010-3235)远程代码执行漏洞、Microsoft Excel公式子流(CVE-2010-3234)远程代码执行漏洞、Microsoft Excel记录解析(CVE-2010-3231)远程代码执行漏洞、Microsoft Excel记录格式解析(CVE-2010-3232)远程代码执行漏洞、Microsoft Excel Lotus 1-2-3工作簿(CVE-2010-3232)远程代码执行漏洞、Microsoft Excel记录解析(CVE-2010-3230)整数溢出漏洞、Microsoft Excel Ghost记录类型

(CVE-2010-3242)远程代码执行漏洞、Microsoft Internet Explorer未初始化内存
(CVE-2010-3331) 远程代码执行漏洞、Microsoft Internet Explorer未初始化内存Word文档
远程代码执行漏洞、Microsoft Internet Explorer未初始化内存 (CVE-2010-3328) 远程代码
执行漏洞、Microsoft Internet Explorer锚点信息泄漏漏洞、Microsoft Internet Explorer
'toStaticHTML' HTML过滤信息泄漏漏洞、Microsoft Internet Explorer HTML过滤
(CVE-2010-3324)信息泄漏漏洞、Microsoft Internet Explorer未初始化内存 (CVE-2010-3326)
远程代码执行漏洞、Microsoft Internet Explorer自动完成信息泄漏漏洞、Microsoft Internet
Explorer CSS特殊字符处理信息泄漏漏洞、Microsoft Internet Explorer跨域 (CVE-2010-3330)
信息泄漏漏洞、Microsoft Windows Media Player内存破坏漏洞、Microsoft MFC库
'UpdateFrameTitleForDocument()' 缓冲区溢出漏洞、Microsoft .NET Framework JIT编译器
优化远程代码执行漏洞、Microsoft Windows嵌入式OpenType字体引擎整数溢出远程代码执
行漏洞、Microsoft Windows COM对象校验远程代码执行漏洞、Microsoft Word未初始化指
针(CVE-2010-2747)远程代码执行漏洞、Microsoft Word (CVE-2010-2748)远程代码执行漏
洞、Microsoft Word索引值处理(CVE-2010-2750)远程代码执行漏洞、Microsoft Word栈处理
(CVE-2010-3214)远程代码执行漏洞、Microsoft Word返回值处理(CVE-2010-3215)远程代码
执行漏洞、Microsoft Word书签处理(CVE-2010-3216)远程代码执行漏洞、Microsoft Word
(CVE-2010-3217)远程代码执行漏洞、Microsoft Word畸形记录值(CVE-2010-3218)远程代码
执行漏洞、Microsoft Word索引值解析(CVE-2010-3219)远程代码执行漏洞、Microsoft Word
记录值解析(CVE-2010-3220)远程代码执行漏洞、Microsoft Word记录值解析
(CVE-2010-3221)远程代码执行漏洞、Microsoft Windows Kernel 'Win32k.sys' 窗口类本地
特权提升漏洞、Microsoft Windows Kernel 'Win32k.sys' 键盘布局本地特权提升漏洞、
Microsoft Windows 'NtUserCheckAccessForIntegrityLevel' 本地特权提升漏洞、Microsoft
Windows SChannel TLSv1远程拒绝服务漏洞、Microsoft Windows远程过程调用子系统本地
特权提升漏洞、Microsoft Windows OpenType字体(OTF)解析特权提升漏洞、Microsoft
Windows OpenType字体(OTF)格式驱动特权提升漏洞。目前，Microsoft在月度例行安全公
告已经同步发布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-2010-02312>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02405>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02403>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02402>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02401>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02396>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02395>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02393>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02391>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02390>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02387>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02385>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02383>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02382>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02380>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02375>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02371>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02363>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02357>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02342>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02406>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02404>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02394>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02392>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02389>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02388>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02386>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02384>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02381>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02379>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02378>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02374>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02370>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02367>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02364>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02362>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02351>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02348>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02345>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02343>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02332>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02330>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02329>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02328>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02326>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02325>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02324>

2、Oracle 多个产品存在安全漏洞

Oracle Siebel 产品、Oracle 数据库、电子商务套件、Fusion Middleware 等 Oracle 产品存在多个安全漏洞。远程攻击者可以利用漏洞获得敏感信息或以应用程序权限执行任意指令。具体漏洞包括：Oracle Fusion Middleware Oracle Fusion Middleware 存在安全漏洞

(CVE-2010-3501)、Oracle Fusion Middleware 存在安全漏洞(CVE-2010-3581)、Oracle Database 作业队列组件存在未明错误、Oracle Fusion Middleware ‘EM Console’ 组件存在错误、Oracle Fusion Middleware 存在多个安全漏洞、Oracle Fusion Middleware ‘Forms’ 组件存在错误、Oracle Fusion Middleware ‘BI Publisher’ 组件存在错误、Oracle Database ‘Core RDBMS’ 组件存在未明错误、Oracle Database ‘XDK’ 组件存在未明错误、Oracle Database ‘OLAP’ 组件存在未明错误、Oracle Database ‘Change Data Capture’ 组件存在未明错误、Oracle Database Java 虚拟机存在未明错误、Oracle Fusion Middleware ‘Perl’ 组件存在未明错误、Oracle Explorer 存在未明安全漏洞、Oracle Communications Messaging Server "Webmail"存在未明安全漏洞、Oracle Primavera P6 Enterprise Project Portfolio Management 存在未明安全漏洞、Oracle Supply Chain 产品 ‘Transportation Management’ 组件存在未明错误漏洞、Oracle Database "Perl"组件存在未明错误、Oracle Supply Chain 的"Agile PLM 组件存在未明错误漏洞、Oracle Database ‘EM Console’ 组件存在未明错误、Oracle Siebel 产品存在未明漏洞 (CVE-2010-2405)、Oracle Siebel 产品存在未明漏洞 (CVE-2010-2406)、Oracle Siebel 产品存在未明漏洞 (CVE-2010-3500)、Oracle Siebel 产品存在多个安全漏洞 (CVE-2010-3502)、Oracle E-Business Suite ‘iRecruitment’ 组件存在未明错误漏洞、Oracle E-Business Suite ‘E-Business Intelligence’ 组件存在未明错误、Oracle E-Business Suite ‘Oracle Territory Management’ 组件存在未明错误漏洞、Oracle E-Business Suite ‘Applications Technology Stack’ 组件存在未明错误漏洞、Oracle Database 企业管理器 GRIP 控件存在未明错误。目前 Oracle 已经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-2010-02347>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02338>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02337>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02335>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02334>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02413>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02400>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02398>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02397>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02352>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02350>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02349>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02344>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02341>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02340>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02336>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02377>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02366>

<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02365>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02361>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02359>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02355>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02410>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02409>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02408>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02407>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02360>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02412>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02411>

3、Sun Solaris 操作系统和 Java 通信套件存在多个安全漏洞

Sun Solaris是一款商业性质的操作系统，Sun Java Communications Suite是一款通信套件。Sun Solaris操作系统和Java通信套件存在多个安全漏洞，允许攻击者以应用程序权限执行任意指令。具体漏洞包括：Sun Java System Identity Manager存在未明安全漏洞、Sun Java Communications Suite的‘Authentication mechanism’组件存在未明错误漏洞、Sun Java Communications Suite的‘Webmail’组件存在未明错误漏洞、Sun Java System Directory Server Enterprise Edition存在未明安全漏洞、Sun Solaris的‘su’组件存在未明错误漏洞、Sun Solaris的‘Kernel/X86’组件存在未明错误漏洞、Sun Solaris的‘InfiniBand’组件存在未明错误漏洞、Sun Solaris的‘ZFS’组件存在未明错误漏洞、Sun Solaris的‘Solaris Zones’组件存在未明错误漏洞。目前Oracle供应商已经发布安全公告修复上述安全漏洞，建议用户尽快下载使用。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02339>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02354>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02356>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02358>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02368>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02369>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02372>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02373>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02376>

4、Moodle网络教学应用程序存在多个安全漏洞

Moodle是一款开放源代码的网络教学应用程序。Moodle存在多个安全漏洞，远程攻击者可以利用这些漏洞获取敏感信息。具体漏洞包括：Moodle存在KSES文本清理漏洞、Moodle存在phpcas模块输入验证漏洞、Moodle存在泄漏用户名漏洞、Moodle存在课程恢复访问控制实现漏洞、Moodle存在Wiki模块漏洞、Moodle存在全局搜索表单的用户输入数据缺少过滤漏洞、Moodle存在默认没有启用会话固定防止功能漏洞。目前Moodle 1.9.8和1.8.9已经修复上述安全漏洞，建议相关用户尽快下载使用。

参考链接: <http://www.cnvd.org.cn/vulnerability/CNVD-2010-02317>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02318>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02319>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02320>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02321>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02322>
<http://www.cnvd.org.cn/vulnerability/CNVD-2010-02323>

小结: 本周, Microsoft 发布的月度例行安全公告称 Windows 操作系统、IE 浏览器、Office 办公套件、Microsoft 服务器软件和 .Net framework 等微软产品中共存在 49 处安全漏洞。Oracle Siebel、Oracle 数据库、电子商务套件、Fusion Middleware 等 Oracle 产品也曝出多个安全漏洞。此外, Sun Solaris 操作系统和 Java 通信套件、Moodle 网络教学应用程序均存在多个安全漏洞。这些漏洞涉及的信息系统和用户群体较为广泛, 对用户的信息安全和公共互联网网络安全构成较为严重的威胁。相关厂商已经发布安全公告或提供解决方案请使用上述软件的相关机构和个人参照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、Oracle 发布安全公告修复了多个漏洞

Oracle 于 10 月 13 日发布安全公告, 修复了包括 Oracle iPlanet Web Server、Oracle Communications Messaging Server、Oracle E-Business Suite、Oracle iPlanet Web Server、Oracle Siebel、Oracle Fusion Middleware 等产品的漏洞。这些漏洞可导致敏感信息泄露、拒绝服务和任意代码执行攻击。建议用户尽快下载补丁程序修复漏洞。

补丁下载链接: <http://www.cnvd.org.cn/patch/1315>
<http://www.cnvd.org.cn/patch/1317>
<http://www.cnvd.org.cn/patch/1319>
<http://www.cnvd.org.cn/patch/1322>
<http://www.cnvd.org.cn/patch/1323>
<http://www.cnvd.org.cn/patch/1324>
<http://www.cnvd.org.cn/patch/1283>
<http://www.cnvd.org.cn/patch/1268>
<http://www.cnvd.org.cn/patch/1269>
<http://www.cnvd.org.cn/patch/1272>
<http://www.cnvd.org.cn/patch/1274>
<http://www.cnvd.org.cn/patch/1298>
<http://www.cnvd.org.cn/patch/1299>
<http://www.cnvd.org.cn/patch/1302>
<http://www.cnvd.org.cn/patch/1303>

<http://www.cnvd.org.cn/patch/1305>
<http://www.cnvd.org.cn/patch/1316>
<http://www.cnvd.org.cn/patch/1318>
<http://www.cnvd.org.cn/patch/1320>
<http://www.cnvd.org.cn/patch/1321>
<http://www.cnvd.org.cn/patch/1249>
<http://www.cnvd.org.cn/patch/1251>
<http://www.cnvd.org.cn/patch/1258>
<http://www.cnvd.org.cn/patch/1260>
<http://www.cnvd.org.cn/patch/1267>
<http://www.cnvd.org.cn/patch/1265>
<http://www.cnvd.org.cn/patch/1262>
<http://www.cnvd.org.cn/patch/1261>
<http://www.cnvd.org.cn/patch/1244>
<http://www.cnvd.org.cn/patch/1246>
<http://www.cnvd.org.cn/patch/1247>
<http://www.cnvd.org.cn/patch/1250>
<http://www.cnvd.org.cn/patch/1253>

本周要闻速递

1、微软发布最大规模补丁包 修复 49 个安全漏洞

据国外媒体报道，微软于美国当地时间周二向全球用户发布 16 个安全补丁包，修补存在于 Windows 操作系统、IE 浏览器、Office 软件、以及企业服务器软件等产品上的 49 个安全漏洞，刷新了微软安全漏洞修补数量的历史记录。新发布的安全补丁包括 4 个高危级别、10 个重要级别，以及 2 个中等级别，分别针对存在于微软产品中的远程代码执行漏洞、信息泄露漏洞以及本地权限提升漏洞等不同类型安全威胁。微软表示，本次发布的安全补丁包，主要针对目前肆虐的“超级工厂”蠕虫病毒，该病毒对电脑的工业控制系统具有巨大的破坏作用，曾于今年夏天入侵伊朗核电站。

参考链接：<http://tech.qq.com/a/20101013/000081.htm>

2、微软称 Windows7 安全机制只为增加黑客攻击时间

温哥华 Pwn2Own 黑客大赛中，黑客不仅将 IE8 浏览器黑掉，而且还成功利用 Firefox、IE 等浏览器绕过了 Windows 7 系统的 ASLR 技术(地址空间布局随机化)和 DEP(数据执行保护)。微软安全专家，IE 小组经理称这两个操作系统安全技术被绕过并不代表 Windows 7 不安全，ASLR 技术的目的是阻止黑客利用代码访问内存地址，DEP 则可以阻止恶意代码在内存中的运行，这两者可以增加黑客攻击系统的时间，是“非常有效的保护机制”。

参考链接：http://tech.ccidnet.com/art/1099/20101019/2216261_1.html

3、微软：上半年被病毒感染的电脑数量在下降

10月15日消息，据国外媒体报道，微软的安全中心报告表明2010年上半年安全漏洞和恶意软件感染的数量有所减少，在严重程度上有所降低。但是，与上六个月相比2010年上半年微软被迫发布了更多的补丁。微软的安全中心报告 volume 9，涵盖一月到六月的数据，它来源于微软工具 Defender, Microsoft Security Essentials, Internet Explorer, Forefront, Bing 和 Malicious Software Removal Tool。与去年下半年相比，易攻击漏洞数量下降了7.9%，严重程度也大大降低，中等程度和高程度的漏洞分别下降了10.7%和9.3%。与去年下半年相比，涉及到个人识别信息数据漏洞的数量下降了46%。源于恶意行为的数据丢失有一半是由于疏忽造成的。同样，报告还带来了一些关于恶意软件的好消息，被微软桌面和反恶意软件清除的被感染电脑下降了13.8%。在2010年四月到六月间微软清理了650万个僵尸网络感染的电脑。比去年同期先比翻了一倍。

参考链接：http://news.ccidnet.com/art/3213/20101015/2213213_1.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