5 “您的计算机安全吗？”—信息安全漏洞公告与处置

CNCERT 高度重视对安全威胁信息的预警通报工作。由于大部分严重的网络安全威胁都是由信息系统所存在的安全漏洞诱发的 ,所以及时发现和处理漏洞是安全防范工作的重中之重。

5.1国家信息安全漏洞共享平台(CNVD)漏洞收录情况

国家信息安全漏洞共享平台（CNVD）自成立以来，共收集整理漏洞信息 26044 个。其中，2010 年新增漏洞 3447 个，包括高危漏洞 649 个（占 19%）、中危漏洞 987 个（占 29%）、低危漏洞 1811 个（占 52%）。各级别比例分布与月度数量统计如图 5-1、图 5-2 所示。在所收录的上述漏洞中，可用于实施远程网络攻击的漏洞有 2919 个，可用于实施本地攻击的漏洞有 513 个。

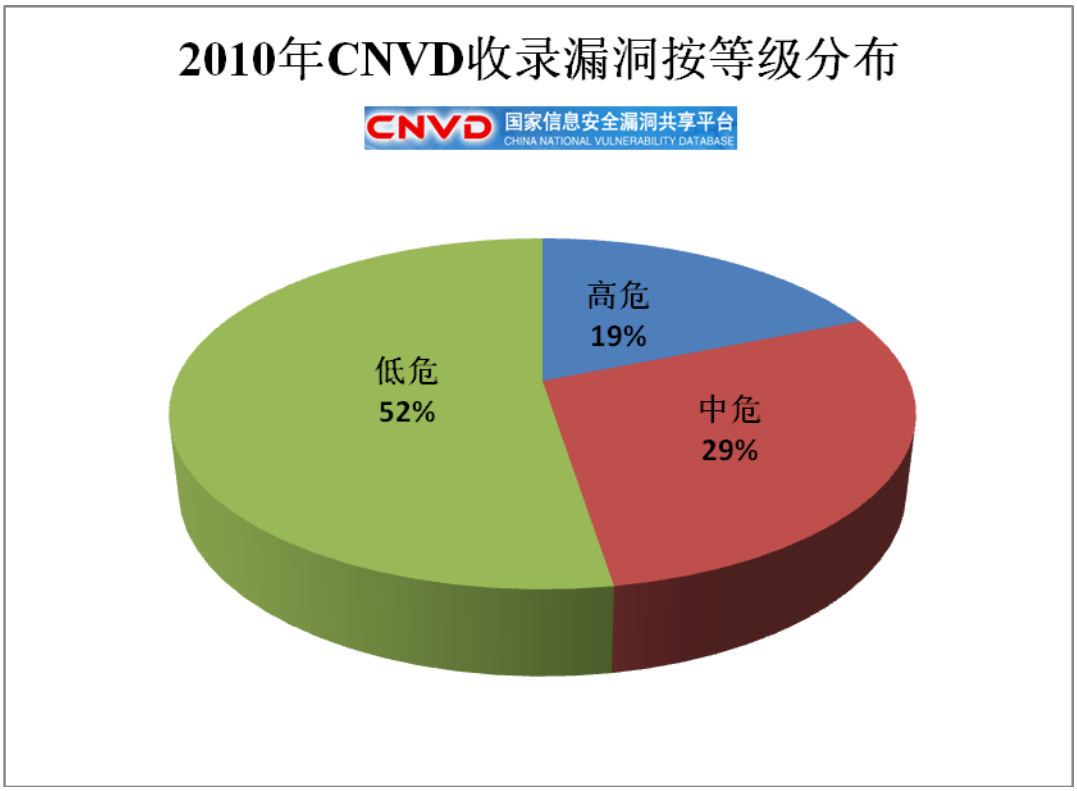

图 5-1　2010 年 CNVD 收录漏洞的级别分布

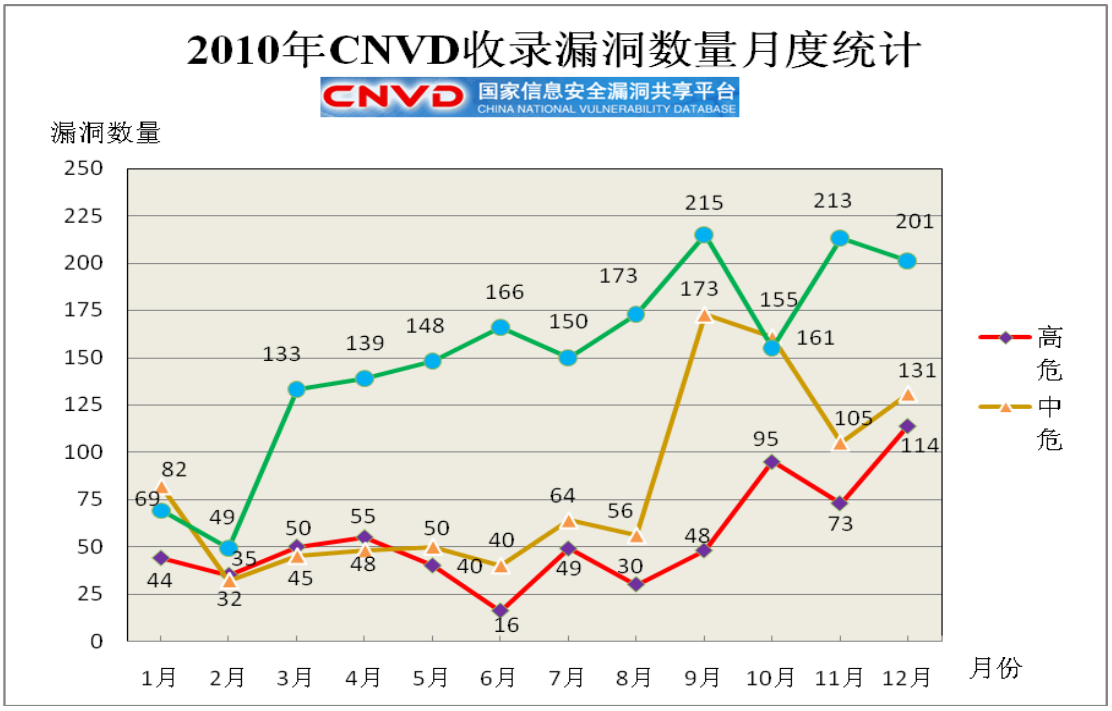

图 5-2 2010 年 CNVD 收录漏洞数量的月度统计

2010 年，CNVD 共收集、整理了 649 个高危漏洞，涵盖 Microsoft、IBM、Apple、Linux、Adobe、Cisco、Mozilla、HP、Google、Sun 等厂商的产品。各厂商产品中高危漏洞的分布情况如图 5-3 所示，可以看出，涉及 Microsoft 产品的高危漏洞最多，占全部高危漏洞的 17%。

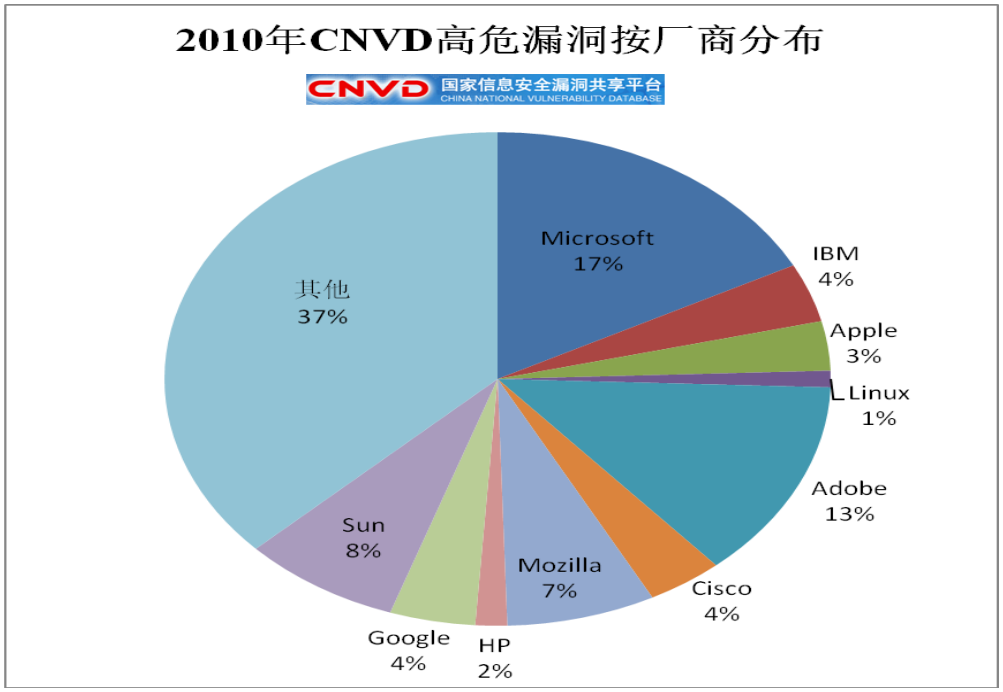

图 5-3　2010 年 CNVD 收录高危漏洞的厂商分布

根据影响对象的类型，漏洞可分为：操作系统漏洞、应用程序漏洞、WEB

应用漏洞、数据库漏洞、网络设备漏洞（如路由器、交换机等）和安全产品漏洞（如防火墙、入侵检测系统等）。如图 5-4 所示，在 CNVD2010 年度收集整理的漏洞信息中，操作系统漏洞占 16%，应用程序漏洞占 62%，WEB 应用漏洞占 9%，数据库漏洞占 4%，网络设备漏洞占 6%，安全产品漏洞占 3%。

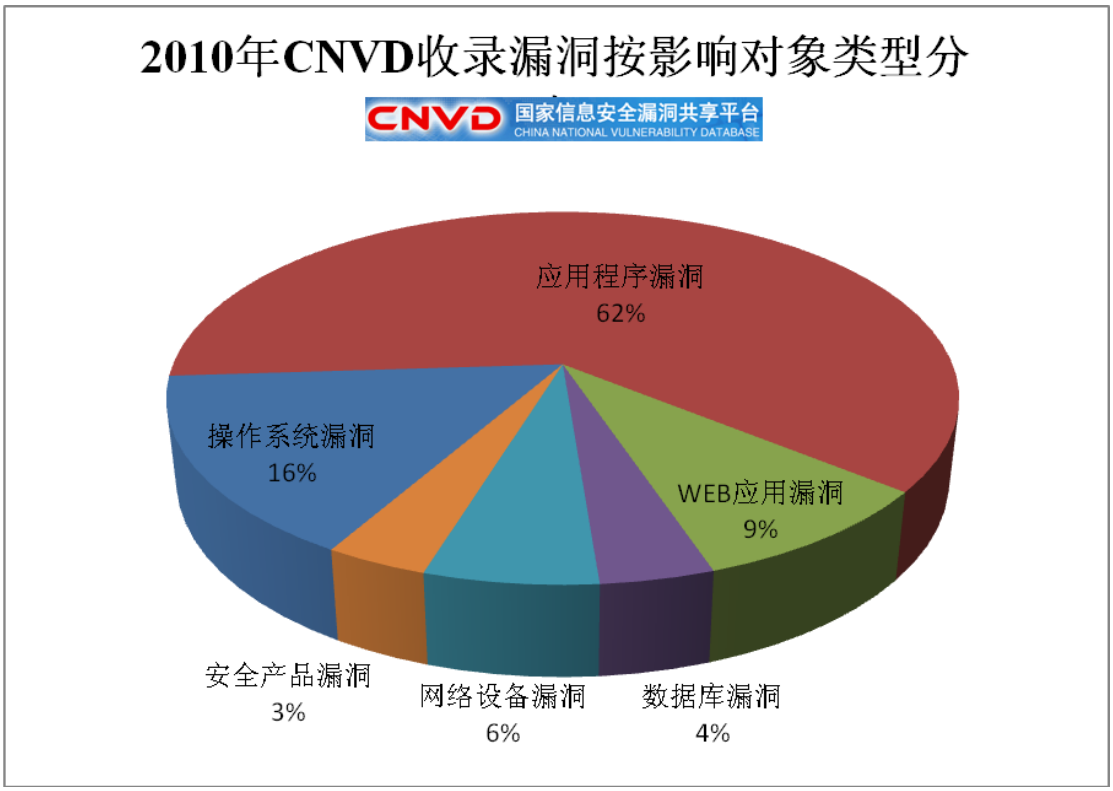

图 5-4　2010 年 CNVD 收录漏洞按类型分类统计图

CNVD 会对收录的漏洞进行验证，并掌握一些仅在 CNVD 成员单位中知晓、未通过互联网公开披露的攻击代码。CNVD 通过验证和测试攻击代码，会对漏洞带来的危害进行较为全面的研判。2010 年，CNVD 共进行了 471 次验证，其中比较重要的包括 Maxthon 浏览器 CSS 远程拒绝服务漏洞、Microsoft Internet Explorer CSS 标签远程代码执行漏洞、CMNC-200 IP 摄像机存在拒绝服务攻击漏洞、Microsoft Internet Explorer CSS 内存损坏漏洞、XOOPS 任意文件删除和 HTTP 头注入漏洞、Microsoft Windows #GP 陷阱处理器本地权限提升漏洞、Android 2.0-2.1 下 Webkit 缺陷引发的反弹 Shell 漏洞、Microsoft IE 畸形对象操作内存破坏漏洞、Microsoft Windows 快捷方式'LNK'文件自动文件执行漏洞、Research In Motion 黑莓设备软件跨域信息泄漏漏洞、GNU glibc 动态链接器'$ORIGIN'本地特权提升漏洞、Adobe Illustrator 非信任搜索路径漏洞、Cisco IOS IGMPv3 存在拒绝服务漏洞、Lynx 浏览器'convert_to_idna()'函数存在远程堆缓冲区溢出漏洞、海海软件 PDFReaderOCX ActiveX 控件"URL"属性缓冲区溢出漏洞、Spring Framework "classLoader" 代码执行漏洞、IBM WebSphere

Application Server SIP 日志信息泄漏漏洞、华为 EchoLife HG520c AutoRestart.html 页面远程拒绝服务漏洞、MyBB set_common_header()邮件 BCC 头注入漏洞等。

漏洞中最危险的是零日漏洞，一旦针对这些高危漏洞的攻击代码在补丁发布之前被公开或被不法分子知晓，就可能被利用来发动大规模网络攻击。2010 年 CNVD 共收录了 340 个零日漏洞，涉及服务器系统、操作系统、数据库系统以及应用软件等。

2010 年，CNVD 共收录漏洞补丁 2310 个，并为大部分漏洞提供了可参考的解决方案，提醒相关用户注意更新，做好系统加固和安全防范工作。CNVD 按月发布的漏洞补丁数量如图 5-5 所示。

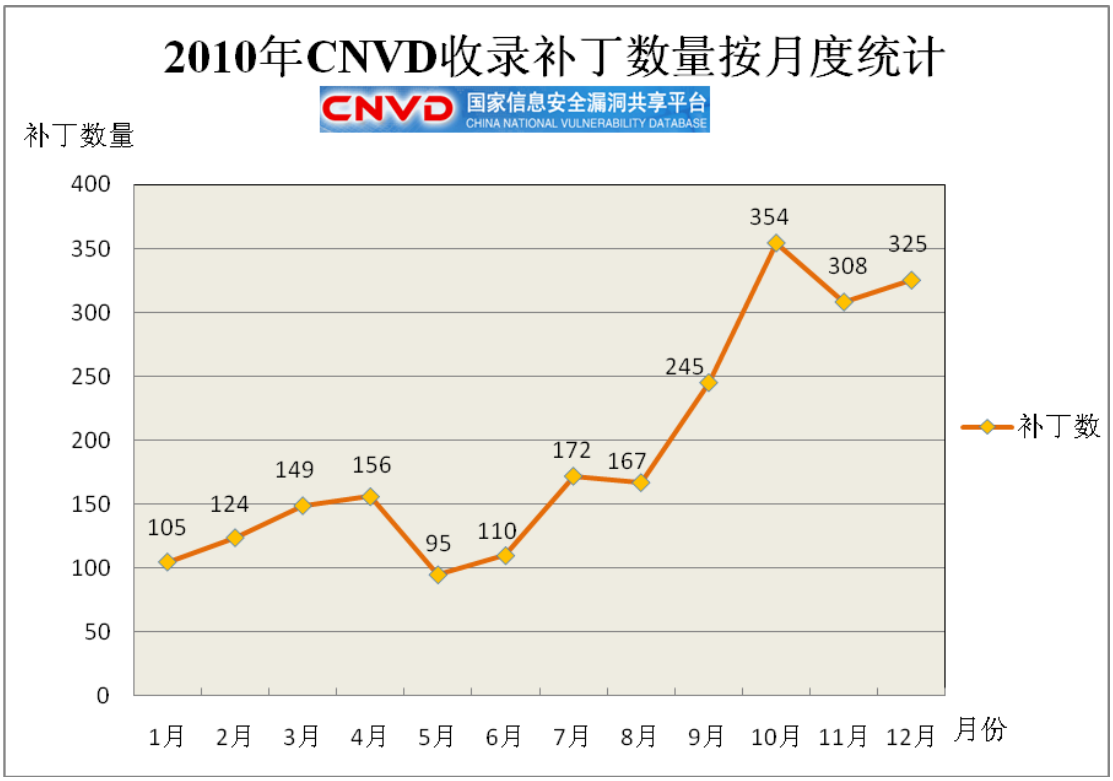

图 5-5 2010 年 CNVD 按月发布的补丁数量

5.2 高危漏洞典型案例

■ 论坛建站软件 Discuz!高危漏洞

2010 年 1 月初，Discuz!论坛建站软件被披露存在一个高危漏洞。Discuz!是康盛创想（北京）科技有限公司基于 php 开发的的论坛建站系统，在国内外的应用均非常广泛。 经 CNVD 调查分析，因 Discuz！7.1 与 7.2 版本的后台代

码中showmessage函数所调用的$scriptlang参数在默认安装的情况下未经初始化，攻击者以论坛普通用户身份登陆后，可以执行特殊构造的 PHP 命令取得网站管理权限，进而窃取用户私密信息。在该漏洞被披露的同时，互联网上迅速出现了针对其的攻击代码，一些使用 Discuz!软件建设的知名 BBS 论坛受到了攻击，据康盛创想公司估计，国内约有 10 余万论坛网站受到威胁。针对上述情况，康盛创想公司紧急发布漏洞补丁；CNCERT 和 CNVD 则向通信行业、社会公众发布紧急安全公告，提醒广大用户下载补丁对网站进行加固，并检查服务器日志，及时发现可能的入侵痕迹。

■ MySQL yaSSL 库证书解析远程溢出漏洞

2010 年 1 月底，数据库系统软件 MySQL 被披露存在一个零日高危漏洞。CNVD 研究分析发现：该漏洞存在于 MySQL 自带的 yaSSL 库中。MySQL 在编译时，如加入对 SSL 的支持，往往会启用 yaSSL 库。yaSSL 库在解析证书文件时，对证书的相关属性参数未做安全检查。攻击者可构造畸形数据导致 yaSSL 库发生栈缓冲区溢出，进而可执行指定命令，控制数据库系统。更为危险的是，攻击者发动攻击是在与数据库系统建立连接会话的初始阶段，不需要进行证书身份认证，使得攻击成功的概率大大增加。受该漏洞影响的 MySQL 版本包括 5.5、5.1 和 5.0.x，这些版本在各部门、各行业信息系统应用较为广泛。黑客极易利用此漏洞窃取数据库中存储的私密信息。对于该漏洞，CNCERT 发布了紧急安全公告和信息通报，提醒 MySQL 用户注意采取防护措施，并给出了在官方补丁方案发布前的临时防范措施。

■ Microsoft IE 对象重用远程攻击漏洞

3 月 10 日凌晨，微软公司发布安全公告称 IE 浏览器存在一个零日高危漏洞（Microsoft Security Advisory，981374）。在漏洞由官方发布之前， CNVD 已经发现并掌握了漏洞的详细情况，并于 3 月 2 日向微软公司通报。CNCERT 还组织 CNVD 成员单位（知道创宇公司、奇虎 360 公司）对漏洞完成了测试验证，发现 IE 浏览器在解析页面时，如页面使用 Javascript 脚本语言对<body>标签进行特定操作，则会引发错误异常，进而可执行任意指定代码。黑客利用该漏洞可通过网页挂马、邮件挂马等方式发动攻击，控制用户计算机。受该漏洞影响的版本包括 IE 6 和 IE 7，而 IE 5 和 IE 8 不受影响。鉴于 3 月 10 日微软公司发布的安全公告中并未包含漏洞补丁，且该漏洞极易被利用、影响范围广， CNVD 发布了紧急公告，建议各单位提高警惕并做好用户安全防范工作。

■ 暴风影音播放器 M3U 文件处理远程溢出漏洞

2010 年 5 月初，CNVD 成员单位发现暴风影音播放器存在 M3U 文件处理相关的高危远程溢出漏洞。M3U 为音频文件的列表文件格式，用户使用播放软件打开 M3U 格式文件时，播放软件根据 M3U 的记录找到网络地址进行在线播放，暴风影音播放器在处理 M3U 文件时存在边界检查错误，从而导致了这个溢出漏洞。攻击者可以利用该漏洞通过欺骗用户点击 M3U 播放文件或通过网页挂马方式，发起攻击，进而达到控制用户主机的目的。对于该漏洞，CNVD 及时发布了安全公告，提醒暴风影音用户注意加强防范，并给出具体建议措施。

■ Web 服务软件 nginx 高危漏洞

2010 年 5 月中旬，一款应用广泛的 Web 服务软件 nginx 被披露存在一个高危漏洞，黑客利用该漏洞可以轻易攻陷网站服务器，获得网站的管理权限。当时互联网上已经出现大量针对该漏洞的攻击程序，据估计采用该服务软件的网站服务器数以百万计，国内许多门户网站和交友社区网站均采用该软件提供网站服务。该漏洞披露后，CNVD 一直密切关注该漏洞事件的动态情况，积极协调国内安全企业协助进行监测，并通过 CNCERT 通报工作平台向政府和重要信息系统部门发布紧急通报，提醒各单位、各部门加强防范，认真检查所管理的网站服务器是否存在该漏洞，避免给黑客可乘之机。

■ Microsoft Windows 快捷方式'LNK'文件自动文件执行漏洞

2010 年 7 月，Microsoft Windows 的快捷方式'LNK'文件曝出重大漏洞。Microsoft Windows 支持使用 LNK 文件对本地文件进行引用，点击 LNK 文件本质上与点击快捷方式目标文件相同。Microsoft Windows 不正确处理 LNK 文件，特殊构建的 LNK 文件可使 Microsoft Windows 自动执行由快捷方式文件指定的代码，该指定代码可驻留在 USB 驱动、CD-ROM、本地或远程文件系统等其它位置，Windows 资源管理器等显示文件图标的其他应用程序均可作为此漏洞的攻击媒介。该漏洞以其巨大的影响范围和极低的利用复杂度，带来严重的信息安全威胁，甚至也被攻击工业控制系统的"震网病毒"所利用。CNVD 就该漏洞发布了紧急安全公告，提醒广大 Windows 用户注意加强防范措施，并在微软发布安全补丁提醒公众及时进行升级加固，消除漏洞威胁。

■ IBM 公司 Lotus Domino/Notes 群件平台漏洞

2010 年 10 月，CNVD 对美国 IBM 公司 Lotus Domino/Notes 群件（简称 Domino 群件）平台密码散列泄露漏洞进行了分析，认为攻击者利用该漏洞可以

还原强度不足的用户密码，从而取得相关用户的全部邮件信息。Domino 群件是IBM 公司开发的一个基于 Web 的协同办公软件包，广泛应用于各个行业，它可以运行在 Windows、Unix 等多种操作系统平台上。该系统在使用默认设置的情况下存在密码散列泄露漏洞，攻击者可以远程访问保存有大量邮件地址信息的Domino 群件后台数据库文件（names.nsf），从中得到全部用户的登录名、邮件地址等信息，进而利用系统设计缺陷远程获取全部用户密码的散列值，然后通过暴力破解还原强度不足的用户密码。如果管理员密码被还原，攻击者便可获得服务器系统的控制权。早在 3 月 9 日，IBM 公司便发布安全公告称 Domino 群件系统存在 HTTP 密码散列泄露问题，4 月份美国 Digital Security 公司发布了针对该漏洞的攻击教程，详细描述了该漏洞的利用方法，并提供了自动化的攻击脚本，经 CNVD 验证确认该攻击方法有效。针对该漏洞，IBM 给出了修改系统默认配置、加强目录访问控制、增加用户密码复杂度的临时解决方案，有效降低了漏洞被利用的风险，但没有在后续产品更新中进行强制修复。因此，受 Domino 群件管理配置相对复杂、漏洞及修复方法宣传不足等因素的影响，目前仍有大量用户选择使用默认配置并处在漏洞威胁之下，面临严重的失泄密风险。CNCERT 和CNVD 就该漏洞及时向政府和重要信息系统部门及通信行业发布了通报预警，提供了切实有效的解决方案，并协助电力、银行等重点行业的十余个部门完成了漏洞的处置工作。

■ Android 2.0-2.1 下 Webkit 缺陷引发的反弹 Shell 漏洞

2010 年 11 月，CNVD 成员单位发现 Android 存在由 Webkit 缺陷引发的反弹 Shell 漏洞。Android 是一款基于 Linux 平台的开源手机操作系统；WebKit 是一个开源的浏览器引擎内核。WebKit 处理浮点数据类型时存在输入验证漏洞，用户访问恶意网站会导致浏览器意外终止或执行攻击者特定构造的程序代码。漏洞被披露时，互联网上已经出现了针对其的攻击程序，而 Android 官方没有对此漏洞发布相关补丁或更新程序，但 Webkit 官方已经修补了此漏洞。CNVD 通过发布安全公告，建议用户及时下载新版 Webkit 内核的手机浏览器或使用其他内核的手机浏览器以避免该漏洞引发信息安全事件。

■ 工业控制系统软件 KingView 缓存区溢出漏洞

2010 年 11 月 26 日，CNVD 接到国外网络安全组织投诉，称北京亚控科技有限公司(简称亚控公司)的软件产品 Kingview 6.5.3 被发现存在一个安全漏洞。Kingview 6.5.3 是 Windows 平台下用于工业自动化的过程控制和管理监控软件，其同步历史数据的服务端口的监听进程在处理数据时未做好安全控制，攻击者通

过向服务端口发送特定构造的数据包会使得服务崩溃或实现溢出获得操作系统主机管理权限。鉴于该软件广泛应用于机械、机电、电力、水处理等行业企业，CNVD 将此漏洞安全级别定义为高危。针对该漏洞，CNVD 启动了高危漏洞的紧急处置机制，向亚控公司通报技术分析结果，督促其推出修复补丁程序，并协调国内相关机构及时进行系统安全加固。

■ Microsoft IE CSS 内存损坏漏洞

圣诞前夕，微软发布了关于 IE 浏览器存在高危零日漏洞的安全公告，称攻击者可利用该漏洞实施网页挂马等攻击活动，进而达到控制用户主机的目的，对广大互联网用户构成严重的信息安全威胁。经 CNVD 调查分析，该漏洞为 HTML 解释器模块的动态链接库文件 mshtml.dll 在处理包含各种“@import”规则的参考 CSS(层叠样式表)文件的网页时，会导致一个名为“use-after-free”的页面文件处理错误。利用该漏洞，攻击者可通过构造特定网页使得 IE 浏览器执行其中嵌入的恶意代码，这就是通常所说的“网页挂马攻击”。受此漏洞影响的 IE 浏览器产品包括 IE6、7、8 三个版本。公告发布时，针对此漏洞的攻击代码已经在网上出现，而且这些攻击代码能够使 ASLR（Address Space Layout Randomization，地址空间布局随机化）和 DEP（Data Execution Prevention，数据执行保护）等微软 Windows 操作系统的保护机制失效，对广大 Windows 用户的安全构成严重威胁。CNVD 及时就该漏洞发布了安全公告，提醒广大用户注意采取防范措施，避免因该漏洞引发信息安全事件。