5 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 2009 年成立以来，共收集整理漏洞信息 35032 个。其中，2011 年新增漏洞 5547 个，包括高危漏洞 2164 个（占 39.0%）、中危漏洞 2529 个（占 45.6%）、低危漏洞 854 个（占 15.4%）。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 4692 个，可用于实施本地攻击的漏洞有 559 个。

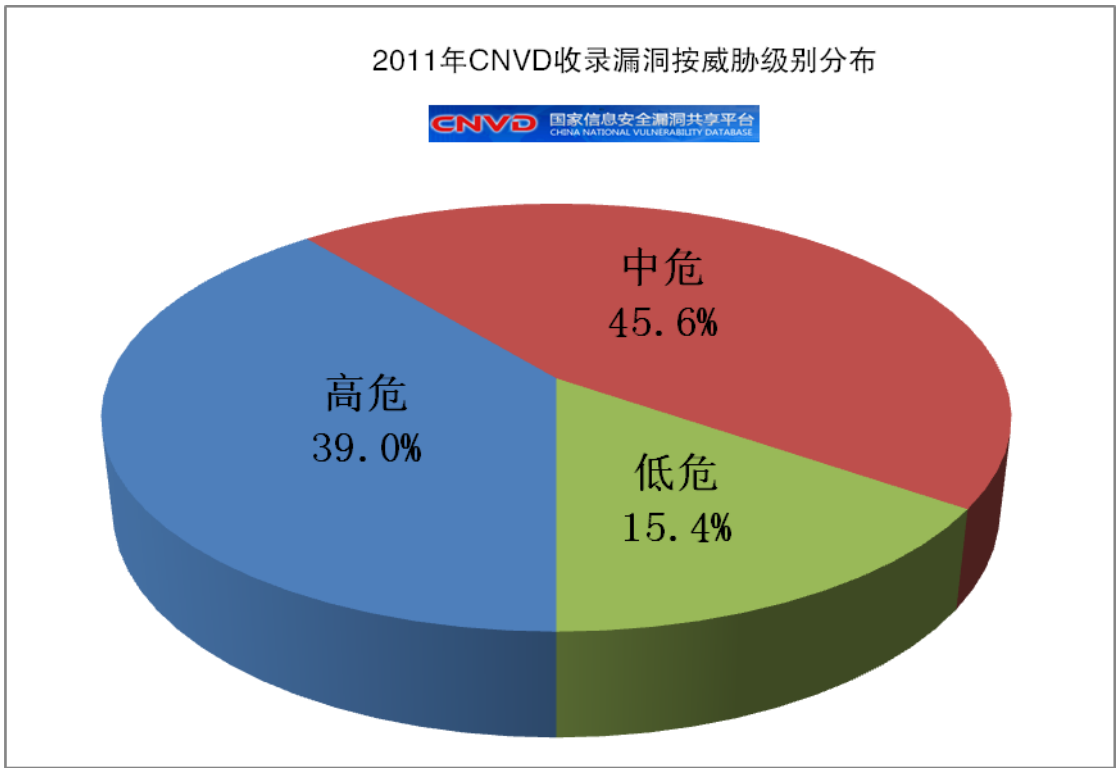

图 5-1 2011 年 CNVD 收录漏洞按威胁级别分布

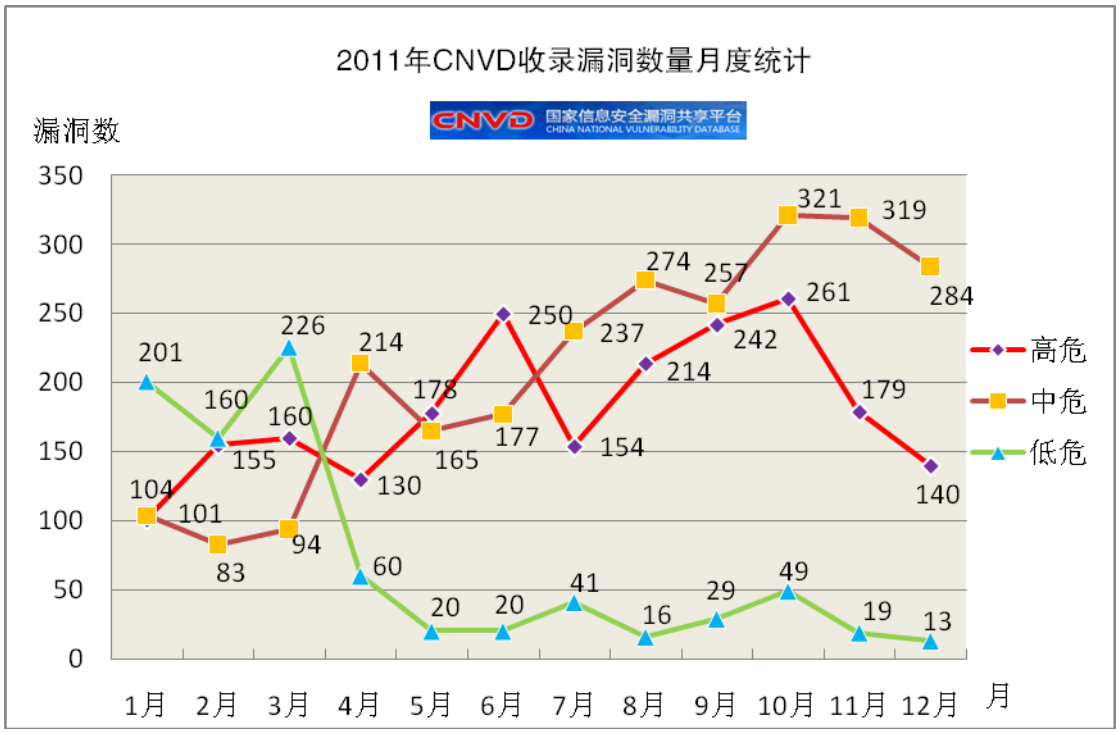

图 5-2　2011 年 CNVD 收录漏洞数量月度统计

2011 年，CNVD 共收集、整理了 2164 个高危漏洞，涵盖 Microsoft、IBM、Apple、WordPress、Adobe、Cisco、Mozilla、Novell、Google、Oracle 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 Apple 产品的高危漏洞最多，占全部高危漏洞的 7.6%。

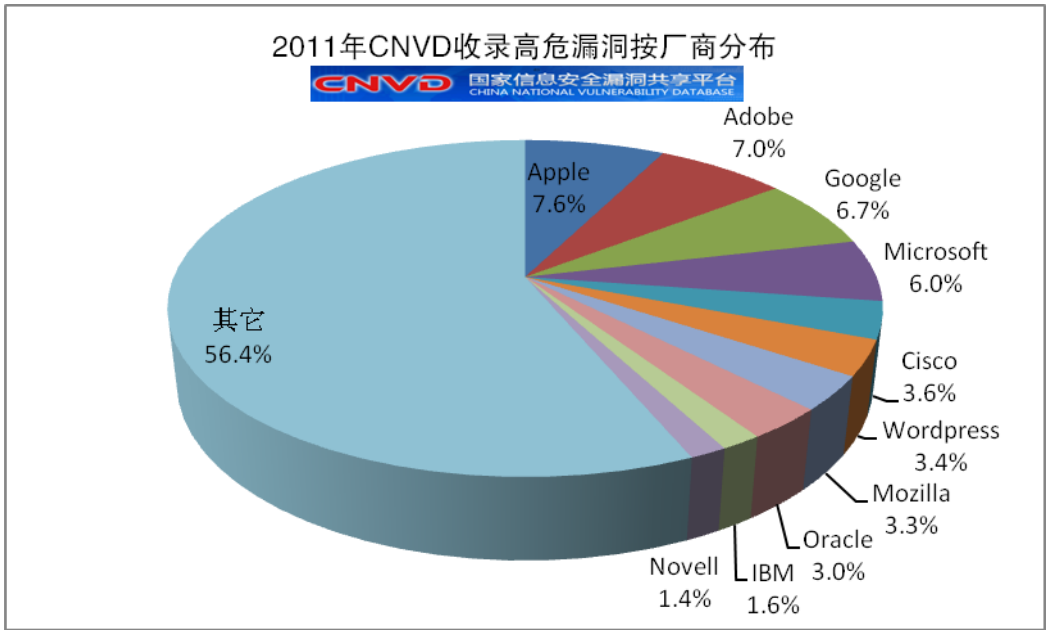

图 5-3　2011 年 CNVD 收录高危漏洞按厂商分布

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 CNVD 2011 年度收集整理的漏洞信息中，操作系统漏洞占 8.8%，应用程序漏洞占 62.5%，WEB 应用漏洞占 22.7%，数据库漏洞 1.1%，网络设备漏洞占 3.7%，安全产品漏洞占 1.2%。

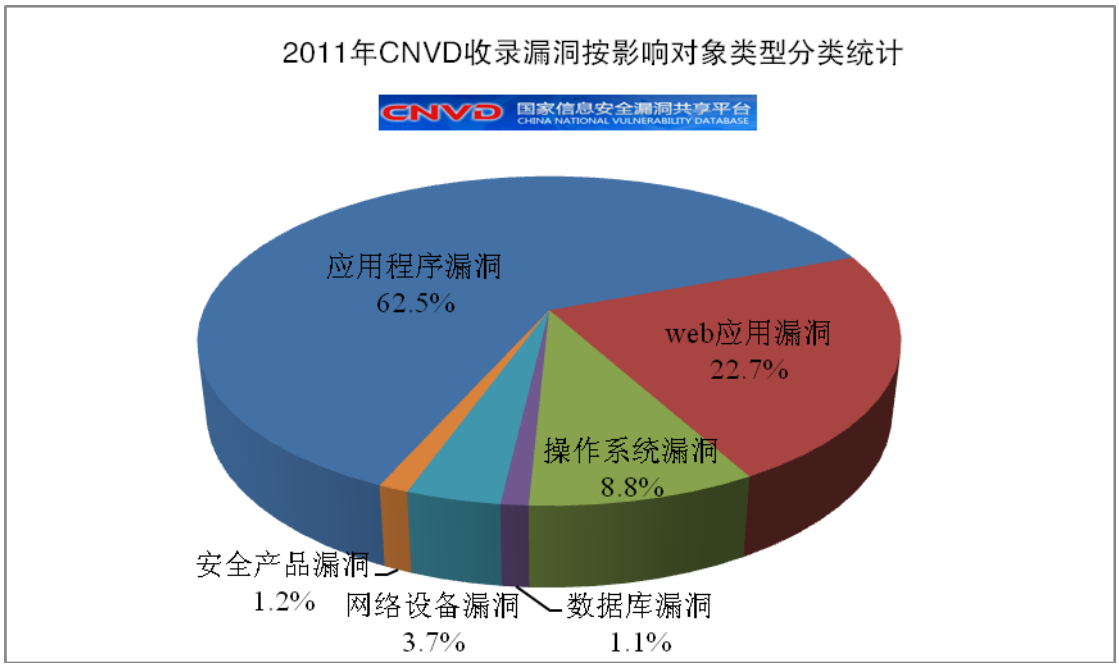

图 5-4　2011 年 CNVD 收录漏洞按影响对象类型分类统计

CNVD 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，对漏洞带来的危害进行了较为全面的分析研判。2011 年，CNVD 共进行了 1340 次验证，其中比较重要的包括 ForceControl 6.1 WebServer URI 请求堆缓冲区溢出漏洞、pNetPower 6.1 AngelServer UDP 数据包堆缓冲区溢出漏洞、心海软件学校心理管理系统 cookie 伪造漏洞、深信服 SSL_VPN 系统控制台验证绕过漏洞、WanHu ezEIP 注入漏洞、NJStar Communicator MINISMTP.exe 服务器堆栈缓冲区溢出漏洞、EC_word 企业管理系统注入漏洞、Discuz! X2 SQL 注入漏洞、pNetPower 6.1 AngelServer UDP 数据包堆缓冲区溢出漏洞补丁衍生拒绝服务漏洞、H3C ER 系列路由器产品验证绕过漏洞、网赢企业网络营销平台注入漏洞、TurboCMS Java 内容管理系统注入漏洞、Apache 远程拒绝服务漏洞、ISC BIND 递归查询远程拒绝服务漏洞、信达证券“牵牛花”系统 SQL 注入漏洞、卓讯智能化网站管理系统 EmteEasySite 多个安全漏洞、宁志学校网站管理系统 SQL 注入漏洞、MyBB MyTabs 插件'tab'参数 SQL 注入漏洞、Nginx %00 空字节执行任意代码(php)漏洞、360eshop 文件上传漏洞等。

漏洞中较危险的是零日漏洞，一旦针对这些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。2011 年 CNVD 共收录了 1340 个零日漏洞，主要涉及服务器系统、操作系统、数据库系统以及应用软件等。

2011 年，CNVD 共收录漏洞补丁 3707 个，并为大部分漏洞提供了可参考的解决方案，提醒相关用户注意做好系统加固和安全防范工作。CNVD 发布的漏洞补丁数量按月度统计如图 5-5 所示。

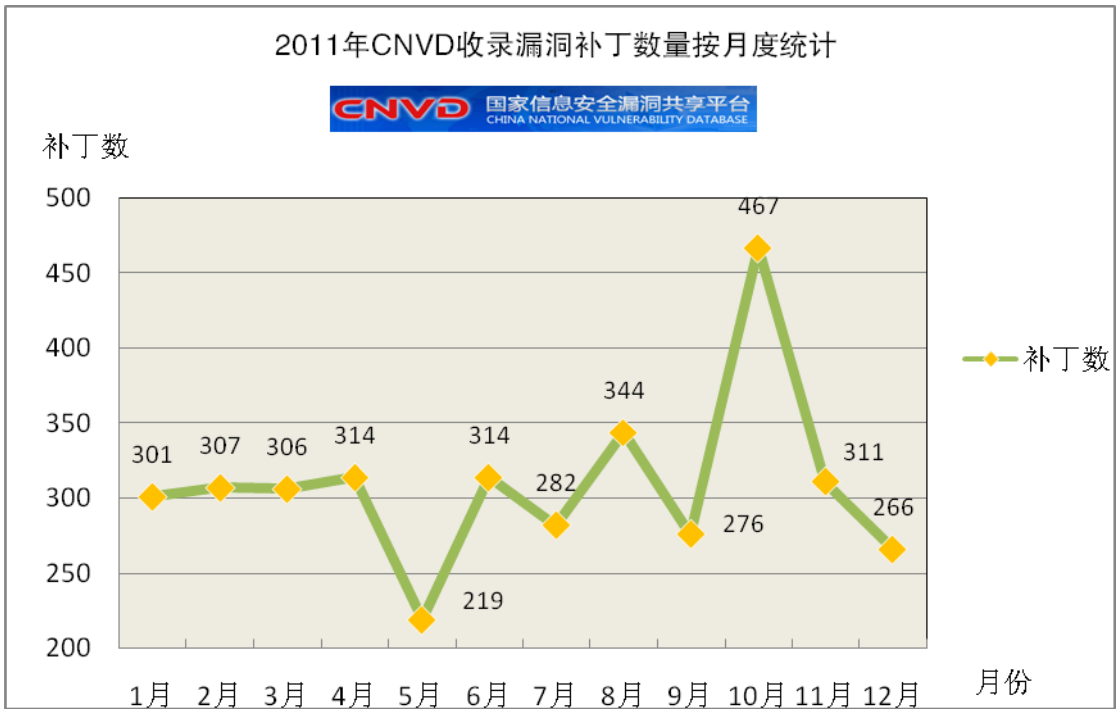

图 5-5　2011 年 CNVD 收录漏洞补丁数量按月统计

5.2 高危漏洞典型案例

■ 亚控公司工业系统监控软件高危漏洞

2011 年 1 月初，北京亚控科技有限公司（简称亚控公司）发布的 HMI/SCADA 系列产品中的 Kingview 6.5.3 组态软件被披露存在一个安全漏洞。该软件主要用于工业自动化的过程控制和管理监控。根据亚控公司提供的客户列表，该软件目前主要应用于国内机械、机电、电力、水处理等行业企业。根据技术分析结果，Kingview 6.5.3 部署在 Windows 操作系统平台上，开启了一个服务端口，用于历史数据同步。由于其服务端口监听进程在处理数据过程中未做好安全控制，攻击者通过向服务端口发送特定构造的数据包导致服务崩溃或实现溢出，从而 获得操作系统主机管理权限。受该漏洞影响的产品运行操作系统有：Windows XP SP1,

SP2, SP3 和 Server 2003。3 月初， CNVD 获知该软件存在另一高危漏洞，受影响的软件版本包括 Kingview 6.5.2 和 6.5.3。CNVD 第一时间对漏洞的真实性进行了验证，并将相关情况通报亚控公司，督促其做好国内外客户的漏洞修复工作。3 月 9 日，亚控公司完成了对漏洞的技术分析，并于 3 月 10 日发布了官方补丁程序。

■ 域名系统软件 ISC BIND 高危漏洞

2 月 23 日，ISC 发布了域名解析服务器软件 BIND 存在的一个高危漏洞，该漏洞可被利用发起远程拒绝服务攻击。CNVD 在漏洞公布之前获知了相关情况，并对漏洞进行了跟踪分析，认为该漏洞可能对国内众多采用相应版本软件的域名服务器构成较为严重的威胁，综合评级为“高危”。经分析， BIND 9.7.1、9.7.2 在处理 IXFR（Incremental zone transfer，增量区域传输）时会在一个小的时间窗口内将其区域内存数据库（in-memory zone database）锁定。如果在该时间窗口内 BIND 服务器再次收到查询请求，则会引起死锁，导致服务器无法响应正常的请求，从而造成拒绝服务。向 BIND 服务器发起的查询请求速率和更新频率越高，则发生拒绝服务的可能性越大。

4 月初，根据中国互联网络信息中心（CNNIC）报告，BIND 9.6-ESV-R3 及之前版本存在一个零日拒绝服务漏洞，该漏洞主要涉及递归服务器对.com 域名的普通查询（非 DNSSEC，即查询的 CD 位＝0）的情形。查询结果可能导致返回 SERVFAIL 应答（即服务错误），根据相关测试出现错误的比例约为 50%。但该漏洞对于.com 域名的 DNSSEC 查询（即查询的 CD 位＝1）没有影响。在 BIND 软件缺省配置开启 DNSSEC 验证功能的情况下，由于大多数 DNS 查询为非 DNSSEC 查询，因此该漏洞对国内使用 BIND 软件提供的递归解析服务有可能造成影响。

6 月下旬，CNVD 获知 BIND 9 存在一个安全漏洞，在特定条件下会导致采用 BIND 9 软件的递归解析服务器拒绝服务。根据 CNNIC 验证情况，由于采用 BIND 9 相关版本软件的递归服务器不能正确处理带有大 RRSIG 资源记录集合的否定应答并进行缓存，当攻击者掌握一台开启 DNSSEC 签名功能的权威服务器，在其区域文件中设置较大的 RRSIG 资源记录集合，然后向递归服务器发送可引发指定权威服务器返回否定应答的 DNSSEC 查询请求，会导致用于递归服务的 BIND 软件 named 进程出错，无法提供正常解析服务。受影响的 BIND 9 版本包括 9.4-ESV-R3 及之后版本、9.6-ESV-R2 及之后版本、9.6.3、9.7.1 及之后版本、9.8.0 及之后版本，其中 9.6.2-P3 不受影响。此外，漏洞与递归服务器是否启用

DNSSEC 查询和验证功能无关。

CNVD 获知相关漏洞信息并验证后，及时发布了紧急安全公告和信息通报，提醒相关用户注意采取防护措施，及时升级软件，避免受到安全影响。

■ 三维力控公司 pNetPower 6.1 高危漏洞

5 月初，pNetPower 6.1 被披露存在高危堆缓冲区溢出漏洞，pNetPower 是北京三维力控科技有限公司推出的一款电力版监控组态软件。在 AngelServer.exe 进程中，对 UDP 包的监测处理未能充分检查边界，攻击者可以利用这一漏洞进行拒绝服务攻击或远程执行任意代码。CNVD 第一时间联系三维力控公司通报了该漏洞情况，该公司立即发布了相应的补丁程序。

9 月底，pNetPower 6.1 堆缓冲区溢出漏洞的补丁被披露存在一个衍生拒绝服务漏洞。由于该补丁中对关键参数未进行 SEH 保护，有可能诱发 AngelServer.exe 进程崩溃，导致攻击者可以利用该漏洞发起远程拒绝服务攻击。CNVD 将此漏洞综合评级定义为“高危“，并提醒 pNetPower 6.1 用户及时关注厂商提供的补丁，更新软件，避免引发漏洞相关的安全事件。

■ Microsoft Word 存在远程代码执行零日漏洞

6 月中旬，国外安全研究机构 Protek Research Lab 披露 Microsoft Word 存在一个远程代码执行零日漏洞。该漏洞是由于 Microsoft Word 文档中的某些参数可被当作指针使用造成的。攻击者可构造嵌入恶意程序的特定文档诱使用户点击来触发此漏洞，此外，还可通过构造恶意网页（即网页挂马）的方式发起远程攻击。一旦攻击成功，攻击者可以执行任意代码，甚至取得主机操作系统管理权限。漏洞主要影响 Microsoft Word XP 和 2002 版本，且在互联网上已经出现了相关攻击代码。CNVD 提醒广大 Microsoft Word 用户随时关注厂商主页获取修补程序，同时不要打开不明来源的 Word 文档以及网页链接，避免引发漏洞相关的网络安全事件。

■ 万户公司网站内容管理系统 WanHu ezEIP 注入漏洞

6 月 30 日，CNVD 发布了关于广州万户网络技术公司（简称万户公司）ezEIP 2.0 软件存在 SQL 注入漏洞的公告，攻击者可以利用漏洞发起远程攻击，取得网站管理员口令，并通过后台管理界面执行网站管理操作权限。ezEIP 2.0 网站内容管理系统是由万户公司生产的用于搭建企业级网站的 CMS 软件（即内容管理系统），根据万户公司官方网站公布的客户列表，该产品用户包括境内外多个政府部门、中央企业及相关行业知名企业。漏洞信息发布后，万户公司及时与 CNVD

取得联系，提出了解决方案，并对相关客户进行排查。至 9 月 30 日，根据万户公司反馈的情况，万户公司对采用存在漏洞软件的 20 余家客户进行了跟踪修复。10 月 8 日，CNVD 发布了关于"WanHu ezEIP 注入漏洞(CNVD-2011-06105)"的补丁公告，对万户公司产品 ezEIP 2.0 网站内容管理系统的漏洞修复情况进行了更新。由于漏洞修复涉及软件配置及代码文件更新，需要厂商提供较多的技术支持。CNVD 提醒相关用户及时联系万户公司，做好修复工作，同时注意加强访问控制，禁止外部 IP 访问默认后台管理页面，对有上传文件功能的页面进行目录读写权限控制或进行服务端验证。

■ H3C ER 系列路由器存在安全漏洞

6 月 29 日，CNVD 收录了杭州华三通信技术有限公司生产的 H3C ER 系列企业级路由器存在的验证绕过漏洞（CNVD-2011-06003），攻击者可以利用漏洞发起远程攻击，查看系统配置等敏感信息，甚至可修改配置，重启设备，对基础电信运营企业以及相关企业、个人用户网络安全构成威胁。受影响的产品为 H3C ER3100、ER3200、ER3260、ER5100、ER5200 等多款同系列产品。根据华三公司公布的相关信息，该系列产品主要用于以太网/光纤/ADSL 接入的 SMB 市场和政府、企业机构、网吧等网络环境。CNVD 工作委员会成员单位 CNCERT、绿盟科技、恒安嘉新对漏洞进行了验证。CNVD 于 6 月 24 日联系了杭州华三通信技术有限公司，该公司承认漏洞存在，但其并未按 CNVD 处置流程要求提供技术细节，也未明确漏洞发布时间以及如何做好客户应急服务的计划。CNCERT 发布了紧急安全公告和信息通报，提醒以上产品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。

■ 颖源公司网站内容管理系统 E3 软件高危漏洞

8 月下旬，CNVD 收录了深圳市颖源科技有限公司（简称颖源公司）生产的 E3 CMS2006 网站内容管理系统（简称 E3 CMS 软件）存在的多个安全漏洞。其中，部分漏洞可被利用获得系统管理员权限，影响涉及我国多家政府部门和电信、金融、保险、地产等行业单位。E3 CMS 软件是由颖源公司生产的用于搭建企业级网站的 CMS 软件（即内容管理系统）。根据中国电力科学院研究院信息安全实验室和 CNVD 的测试结果，E3 CMS2006 内容管理系统存在越权访问漏洞和任意文件上传漏洞。受漏洞影响的版本是 E3 CMS 2006 JAVA Build20070618。根据颖源公司官方网站公布的客户列表，该产品用户包括多个政府部门以及电信、金融、保险、地产等领域的知名企业。CNVD 建议相关用户参照上述漏洞情况自行对网站进行 Web 页面漏洞的检测，及时发现存在的安全隐患。

■ 信达证券“牵牛花”网上交易系统多个安全漏洞

8 月初，CNVD 收录了信达证券股份有限公司（简称信达证券）牵牛花网上交易系统（简称牵牛花系统）存在的四个安全漏洞（CNVD-2011-06304、CNVD-2011-06305、CNVD-2011-06308、CNVD-2011-06309）。其中，部分漏洞可被利用获得证券用户的账号和口令以及个人私密信息，并可执行对用户信息的修改操作，威胁到信达证券用户网上交易和财产安全。

牵牛花系统是由信达证券提供给其证券用户的网上服务平台，为用户提供了预约开户、行情浏览、快速交易、持仓管理、研究资讯分析、模拟炒股等功能。此次发现的四个安全漏洞分别为 SQL 注入漏洞、跨站脚本漏洞、跨站请求伪造漏洞和信息修改漏洞。其中，SQL 注入漏洞存在于牵牛花系统的多处页面中，使用普通用户权限即可完成注入攻击，取得后台数据库的敏感信息，进而有可能取得系统管理控制权限；跨站脚本漏洞为反射型跨站脚本漏洞，攻击者可利用发起网页仿冒（即网络钓鱼）或网页挂马攻击；针对跨站请求伪造漏洞，攻击者可构造含有查询语句或嵌入恶意链接的 URL，轻则窃取用户私密信息或进行跳转攻击，严重的可导致服务器拒绝服务；针对信息修改漏洞，攻击者可通过重新组包方式发送编辑请求，可以对任意用户的个人信息进行篡改。

“牵牛花”网上交易系统采用的是 Web 访问模式（B/S），使用该套系统的用户均受到影响。CNVD 及时发布了安全公告和信息通报，提醒相关用户注意检查登录和使用日志，如发现异常情况及时联系信达证券公司。

■ 心海软件心理管理系统漏洞

9 月 26 日，CNVD 知悉北京心海导航科技有限公司（简称心海公司）的心海软件心理系统软件（教委版）存在 cookie 伪造、文件上传等漏洞。攻击者只要获得任一普通用户的 cookie 样式，即可伪造管理员 cookie 取得系统管理权限；此外，系统的文件上传页面，未对用户上传的文件类型进行合法性验证，攻击者可以上传网页木马获得服务器主机的控制权。根据心海公司发布的客户列表，该漏洞可能影响国内数百家高等院校、中小学校及教育机构，包括多所位列“985 工程”、“211 工程”的高等院校。CNVD 启动了高危漏洞的紧急处置机制，向北京心海导航科技有限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 Windows 内核 Word 文件处理远程代码执行漏洞

11 月初，Microsoft Windows 内核被披露存在一个安全漏洞，允许攻击者以内

核上下文执行任意代码。知名木马 Duqu 就利用了该漏洞发起攻击，其安装软件是一个含有恶意程序的 Microsoft Word 文档(.doc)，当打开这个恶意文档时，将会自动执行恶意程序，并安装 Duqu 程序。CNVD 将此漏洞安全级别定义为“ 高危 ”。

■ Schneider Electric 和 Siemens 多个漏洞

12 月初，Schneider Electric（施耐德电气）和 Siemens（西门子）产品被披露存在多个漏洞，包括内存访问、拒绝服务、缓冲区溢出、跨站脚本、目录遍历等。攻击者利用这些漏洞可对 Schneider Electric 和 Siemens 的工业控制系统用户构成严重的威胁。受影响的产品包括 Schneider Electric 公司 Vijeo Historian 4.30 及之前版本、CitectHistorian 4.30 及之前版本和 CitectSCADA Reports 4.10 及之前版本。Schneider Electric（施耐德电气）官方已对存在漏洞的产品发布了补丁并建议所有用户立即进行修复。