

信息安全漏洞周报

2011 年 1 月 10 日-2011 年 1 月 16 日

2011 年第 2 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 116 个，其中高危漏洞 29 个、中危漏洞 22 个、低危漏洞 65 个。上述漏洞中，可利用来实施远程攻击的漏洞有 106 个。经跟踪发现，网上已经出现针对“Newv SmartClient 'NewvCommon.ocx' ActiveX 控件存在多个安全漏洞”、“VideoSpirit Pro/Lite '.visprj'文件缓冲区溢出漏洞”等的零日攻击代码，请使用相关产品的用户注意做好防护措施。本周收录的安全漏洞中，已有 92 个漏洞由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、亚控公司 KingView 存在缓存区溢出漏洞

2010 年 11 月 24 日，CNVD 接收到国外安全专家和安全组织的报告，称北京亚控科技有限公司生产的用于工业系统管理监控的软件产品 kingview 6.5.3 存在一个严重高危漏洞。接到报告后，CNVD 立即对漏洞情况进行了验证，确认该漏洞可被利用，并对相关工业控制系统的运行安全构成严重威胁。11 月 26 日，CNVD 向亚控公司通报漏洞情况，责成其尽快提供解决方案。12 月 15 日，亚控公司在其官方网站发布了漏洞的修复补丁。2011 年 1 月 12 日，CNVD 再次对漏洞危害情况和影响范围进行确认和评估，并督促亚控公司进一步做好国内外客户的漏洞修复工作。

存在漏洞的是亚控公司生产的 HMI/SCADA 系列产品中的 KingView 6.5.3 组态软件，该软件主要用于工业自动化的过程控制和管理监控。从亚控公司提供的客户列表来看，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，部署在 windows 操作系统平台的 Kingview 6.5.3 会开启一个服务端口用于同步历史数据，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会使得服务崩溃或实现溢出，从而获得操作系统主机管理权限。目前，受

漏洞影响的操作系统有：Windows XP SP1、SP2、SP3 和 Server 2003。CNVD 将此漏洞安全级别定义为“高危”，向有关用户提出如下防范建议措施：（1）及时下载亚控公司发布的安全补丁，对系统进行加固；（2）对网络加强管理，尽可能地将与工业控制系统相关的管理控制主机与互联网隔离。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03727>

2、Microsoft 发布公告修复多个安全漏洞

本周，微软发布 2011 年第一个月度例行安全公告，共包含两个安全更新，其中一个安全等级为“严重”，另一个为“重要”。本次发布的安全更新修复了 Microsoft Data Access Components 中两个之前未公开的漏洞：“Microsoft Data Access 组件 ActiveX 数据对象内存破坏漏洞”和“Microsoft Data Access 组件数据源名缓冲区溢出漏洞”，还有 Windows 备份管理器中一个已公开披露的漏洞：“Microsoft Vista BitLocker Drive Encryption API 非信任搜索路径漏洞”，攻击者可以利用这些漏洞实施远程攻击，在用户主机上执行任意代码。受漏洞影响的操作系统包括 Windows 7 在内的多个 Windows 版本，CNVD 提醒广大用户尽快下载安装补丁程序，避免引发漏洞相关的网络安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03675>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03671>

3、Cisco 存在多个安全漏洞

本周，Cisco 的 IOS 操作系统和 Adaptive Security Appliances 安全设备出现了多个安全漏洞。CNVD 收录的 Cisco 漏洞包括：Cisco IOS 会话初始化协议注册器拒绝服务漏洞、Cisco IOS CallManager Express (CME) (CVE-2009-5040)拒绝服务漏洞、Cisco IOS IRC 服务器拒绝服务漏洞、Cisco Adaptive Security Appliance 提供的 SIP 检测功能存在未明漏洞、Cisco Adaptive Security Appliance在迁移后不正确保留 ACL 行为规则漏洞、Cisco Adaptive Security Appliances (ASA) 5500 存在未授权信息泄漏漏洞、Cisco Adaptive Security Appliances (ASA) 5500 系列设备存在未明安全漏洞（CVE-2010-4691、CVE-2010-4692）等。攻击者可以利用这些漏洞获取敏感信息或进行拒绝服务攻击。其中“Cisco Adaptive Security Appliance 提供的 SIP 检测功能存在未明漏洞、Cisco Adaptive Security Appliance 在迁移后不正确保留 ACL 行为规则漏洞、Cisco Adaptive Security Appliances (ASA) 5500 存在未授权信息泄漏漏洞、Cisco Adaptive Security Appliances (ASA) 5500 系列设备存在未明安全漏洞（CVE-2010-4691、CVE-2010-4692）”的安全等级为“高”，目前厂商已发布这些漏洞的补丁程序，CNVD 建议用户及时下载更新，避免引发此漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03709>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03666>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03667>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03668>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03669>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03670>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03672>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03673>

4、Google Chrome 出现多个安全漏洞

Google Chrome 是一款 WEB 浏览器。本周，Google Chrome 出现了多个安全等级为“高危”的安全漏洞。攻击者可以利用漏洞进行拒绝服务攻击或执行任意代码。CNVD 收录的漏洞包括：Google Chrome 处理 speech 存在漏洞、Google Chrome DOM 节点删除之后的处理存在漏洞、Google Chrome 处理视频存在漏洞、Google Chrome 处理锚(anchors)存在漏洞、Google Chrome PDF 格式底纹处理存在漏洞、Google Chrome Vorbis 解码器存在漏洞、Google Chrome 处理 rouge 扩展存在漏洞、Google Chrome 处理 SVG 元素存在漏洞、Google Chrome 处理不匹配的视频帧大小存在漏洞等。目前，Google 已经发布了这些漏洞的补丁程序，CNVD 建议广大用户及时下载更新，避免引发此类漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03744>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03743>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03742>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03741>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03740>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03739>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03738>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03737>

5、Nokia 多媒体播放器播放列表处理缓冲区溢出漏洞

Nokia Multimedia Player 是一款媒体播放程序。Nokia Multimedia Player 处理播放列表文件时存在问题，攻击者可利用此漏洞在受影响的应用程序中运行任意代码。攻击者诱使用户访问经特殊构建恶意的'.npl'文件，可触发此漏洞。目前厂商尚未发布此漏洞的补丁程序，CNVD 提醒广大 Nokia 用户，随时关注厂商主页以获取最新版本。

参考链接：<http://www.cnvd.org.cn/vulnerability/CNVD-2011-03713>

小结：上述漏洞中，北京亚控科技有限公司 KingView 6.5.3 软件产品存在的高危漏洞可对应用该软件进行生产系统管理控制的机械、机电、电力、水处理等行业企业构成严重威胁。Microsoft 发布月度安全公告修复的 Microsoft Data Access Components 中两个未公开的漏洞和 Windows 备份管理器中一个已公开披露的漏洞，以及 Cisco、Google 和 Nokia 等产品出现的安全漏洞对互联网用户的信息安全和网络安全构成较为严重的威胁，请使用上述软件的相关机构和个人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、 HP 发布升级程序,修补了 OpenView Network Node Manager 的多个安全漏洞

HP OpenView Network Node Manager 是一款惠普公司开发和维护的网络管理系统软件,具有网络节点管理功能。本周,HP 发布了多个升级程序用于修复 OpenView Network Node Manager 产品的多个安全漏洞,避免攻击者利用此漏洞在受影响的应用程序中执行任意代码。CNVD 已收录相关补丁,请广大用户及时下载更新,避免引发漏洞相关的安全事件。

补丁下载链接: <http://www.cnvd.org.cn/patch/2551>
<http://www.cnvd.org.cn/patch/2560>
<http://www.cnvd.org.cn/patch/2555>
<http://www.cnvd.org.cn/patch/2559>

本周要闻速递

1. 微软发布 2011 年第一个月度安全公告 暂未修复 IE “圣诞”漏洞

1 月 12 日凌晨,微软公司按惯例发布了本月安全更新,包括 1 个“危急”补丁和 1 个“重要”补丁。但正在被黑客大面积攻击的 IE 浏览器 CSS “圣诞”漏洞仍未得到修复。据悉,IE “圣诞”漏洞最早是在去年圣诞节前曝光,影响 IE6、IE7、IE8 等主流浏览器版本,涉及 90%以上的中国网民。研究人员称,在未来的一段时间中,我们将看到未修复的漏洞被全面攻击的现象,专家建议在微软官方推出补丁修复漏洞之前,用户应当保持计算机杀毒软件为最新状态,从而在一定程度上避免漏洞带来的危害。

参考链接: <http://news.163.com/11/0114/08/6QBJB1I200014JB5.html>

2. Chrome 漏洞发现者获得谷歌颁发的 3133.7 美元奖金

1 月 14 日消息,据国外媒体报道,谷歌给予 Chrome 漏洞发现者 3133.7 美元奖金。获得这笔奖金的研究人员名叫谢尔盖·格拉祖诺夫,格拉祖诺夫的最大发现是 Chrome 浏览器的“对话控制中的一个指针”存在重大安全隐患。谷歌并没有对此漏洞的具体内容做出任何评论。除了格拉祖诺夫发现的重大漏洞外,谷歌也对其他 15 项脆弱点进行了补丁修复,其中的两个脆弱点较为重要。

参考链接: <http://tech.163.com/11/0114/22/6QD3N6FT000915BF.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