

信息安全漏洞周报

2011 年 12 月 19 日-2011 年 12 月 25 日

2011 年第 51 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 107 个，其中高危漏洞 35 个、中危漏洞 69 个、低危漏洞 3 个。上述漏洞中，可利用来实施远程攻击的漏洞有 98 个。本周收录的漏洞中，已有 72 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。本周互联网上出现“Citrix XenDesktop/XenServer 验证凭据信息泄露漏洞”、“mPDF 'filename'本地文件包含漏洞”等的零日攻击代码，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 6 家成员单位报送了本周收录的全部 107 个漏洞，其中包含 3 个原创漏洞，均为来自北京奇虎科技有限公司手机事业部报送的关于 Android 手机管理软件存在的安全漏洞。

各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技、安天实验室报送数量均较多。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	80	0
绿盟科技	41	0
安天实验室	27	0
恒安嘉新	12	0
奇虎 360	3	3
安氏领信	2	0
总计	107（去重）	3

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、Wuzly、Opera Software 等多家厂商的产品，

部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Mozilla	8	7.5%
2	Wuzly	5	4.7%
3	Opera Software	5	4.7%
6	HP	5	4.7%
4	KIWI Image System	4	3.7%
5	Linux	4	3.7%
7	WhatsApp Inc.	3	2.8%
8	Sandoba.de MedienAgentur	3	2.8%
9	Siemens	2	1.9%
10	Microsoft	1	0.9%
11	其它	67	62.6%

表 2 漏洞产品涉及厂商分布统计表

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、Citrix XenDesktop/XenServer 验证凭据信息泄露漏洞

Citrix XenDesktop/XenServer 是 Citrix（思杰）公司开发的一款桌面/服务器虚拟化系统。本周，Citrix XenDesktop 和 XenServer 被披露存在一个信息泄露漏洞，远程攻击者可以利用漏洞以目标用户权限登录系统，获得对用户虚拟桌面的访问权限。目前，互联网上已经出现针对该漏洞的攻击代码，但厂商尚未发布上述漏洞的修补程序，CNVD 提醒广大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/sites/main/preview/ldgg_preview.htm?tid=35588

2、Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 分别是 Mozilla 发布的 WEB 浏览器/新闻组客户端/邮件客户端。本周，Mozilla 发布安全更新，修复上述 Mozilla 产品的多个安全漏洞。远程攻击者可以利用漏洞以应用程序上下文执行任意代码，使应用程序崩溃或获取敏感信息。CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird 远程代码执行漏洞（CNVD-2011-09117）、Mozilla Firefox/Thunderbird/SeaMonkey 越界内存破坏漏洞、Mozilla Firefox/SeaMonkey 空指针引用拒绝服务漏洞（CNVD-2011-09119）、Mozilla Firefox/Thunderbird/SeaMonkey SVG 动画元素信息泄露漏洞、Mozilla Firefox/Thunderbird/S

eaMonkey YARR 库拒绝服务漏洞、Mozilla Firefox/Thunderbird/SeaMonkey 拒绝服务漏洞 (CNVD-2011-09122)、Mozilla Firefox/Thunderbird/SeaMonkey 存在多个内存破坏漏洞 (CNVD-2011-09123)、Mozilla Firefox 层叠样式表(CSS)浏览器历史信息泄露漏洞。其中,除“Mozilla Firefox/Thunderbird/SeaMonkey SVG 动画元素信息泄露漏洞”、“Mozilla Firefox 层叠样式表(CSS)浏览器历史信息泄露漏洞”外,其余漏洞的综合评级均为“高危”。CNVD 提醒相关用户尽快下载补丁更新,避免引发漏洞相关的网络安全事件。

参考链接: http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35651
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35652
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35653
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35654
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35655
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35656
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35657
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35619

3、Linux 产品安全漏洞

Linux 是一款开源的操作系统。本周, Linux Kernel 被披露存在多个安全漏洞。远程或本地攻击者可以利用漏洞以高权限读取敏感数据;或进行拒绝服务攻击,使系统崩溃。CNVD 收录的相关漏洞包括: Linux Kernel 'SG_IO_IOCTL' SCSI 请求特权提升漏洞、Linux Kernel KVM 'create_pit_timer()'函数本地拒绝服务漏洞、Linux Kernel 紧凑循环和不可抢先本地拒绝服务漏洞、Linux Kernel PMC 本地拒绝服务漏洞。其中,“Linux Kernel 'SG_IO_IOCTL' SCSI 请求特权提升漏洞”的综合评级为“高危”。Linux 已经发布上述漏洞的修补程序, CNVD 提醒相关用户尽快下载补丁更新,避免引发漏洞相关的网络安全事件。

参考链接: http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35691
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35692
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35693
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35591

4、HP 产品安全漏洞

本周, HP (惠普) 公司的产品 HP Managed Printing Administration 和 HP Storage Works P4000 Virtual SAN Appliance 被披露存在多个安全漏洞。HP StorageWorks P4000 Virtual SAN Appliance 是一款虚拟化存储虚拟网解决方案;而 HP Managed Printing Administration 则是一款打印管理工具。利用上述产品漏洞,攻击者可以创建或删除任意文件,获取敏感文件信息或执行任意代码。CNVD 收录的相关漏洞包括: HP Managed Printing Administration 远程创建文件漏洞 (CNVD-2011-09166、CNVD-2011-09167)、HP Managed Printing Administration 存在未明漏洞、HP Managed Printing Admini

stration 远程代码执行漏洞、HP StorageWorks P4000 Virtual SAN Appliance 远程命令执行漏洞。其中，“HP Managed Printing Administration 远程创建文件漏洞（CNVD-2011-09167）”、“HP Managed Printing Administration 远程代码执行漏洞”的综合评级为“高危”。目前，HP 已经发布上述漏洞的修补程序，CNVD 提醒相关用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

参考链接：http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35703
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35704
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35706
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35705
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35617

5、Wuzly 产品安全漏洞

Wuzly 是一款用于搭建博客平台的网站内容管理系统。本周，Wuzly 被披露存在多个安全漏洞。攻击者可以利用漏洞进行跨站请求伪造、目录遍历、SQL 注入攻击和跨站脚本等攻击。CNVD 收录的相关漏洞包括：Wuzly 跨站请求伪造漏洞、Wuzly 目录遍历漏洞、Wuzly SQL 注入漏洞、Wuzly 验证机制漏洞、Wuzly 跨站脚本漏洞。其中，“Wuzly SQL 注入漏洞”的漏洞综合评级为“高危”。目前，厂商尚未发布上述漏洞的修补程序，CNVD 提醒广大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/sites/main/preview/ldgg_preview.htm?tid=35634
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35635
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35636
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35637
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35633

更多高危漏洞如表 3 所示，详细信息可根据 CNVD 编号，在 CNVD 官网进行查询。

参考链接：<http://www.cnvd.org.cn/publish/main/52/index.html>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2011-09163	Ubiquiti Networks AirOS 远程命令执行漏洞（CNVD-2011-09163）	高	用户可联系供应商获得最新固件补丁： http://ubnt.com/support/downloads
CNVD-2011-09151	Free Mp3 Player '.mp3'文件远程缓冲区溢出漏洞	高	暂无
CNVD-2011-09140	PLIB 'ulSetError()'函数远程缓冲区溢出漏洞	高	暂无
CNVD-2011-09141	VLC Media Player 'get_chunk_header()'函数内存破坏漏洞	高	VideoLAN VLC media player 1.1.13 已经修复此漏洞，建议用户下载使用： http://www.videolan.org/

CNVD-2011-09133	7-Technologies Interactive Graphical SCADA System 缓冲区溢出漏洞	高	用户可参考如下供应商提供的安全补丁： http://www.7t.dk/igss/igssupdates/v90/progupdatesv90.zip 也可以在 IGSSMaster 应用程序中，选择菜单项 “Information and Support” 并点击 “Update IGSS Software.” 进行自动升级。
CNVD-2011-09138	King View 'HistoryServer.exe' 基于堆的缓冲区溢出漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.kingview.com/news/detail.aspx?contentid=587
CNVD-2011-09150	DotA OpenStats 'id' 参数 SQL 注入漏洞	高	暂无
CNVD-2011-09149	Infoproject Biznis Heroj 存在多个 SQL 注入漏洞	高	暂无
CNVD-2011-09115	IrfanView TIFF 图像文件远程堆缓冲区溢出漏洞	高	IrfanView 4.32 已经修复此漏洞，建议用户下载使用： http://www.irfanview.com/plugins.htm
CNVD-2011-09116	libfpx 'Free_All_Memory()' 函数两次释放远程代码执行漏洞	高	libfpx 1.3.1-1 已经修复此漏洞，建议用户下载使用： http://www.imagemagick.org/download/delegates/

表 3 部分高危漏洞列表

小结：本周，Mozilla 发布安全更新，修复了 Firefox/SeaMonkey/Thunderbird 多款产品中的安全漏洞，远程攻击者可以利用漏洞以应用程序上下文执行任意代码，使应用程序崩溃或获取敏感信息，Linux 操作系统内核被披露存在多个漏洞，构成信息窃取和拒绝服务等安全风险，上述产品对个人用户安全构成较大威胁。

此外，HP 应用软件、Wuzly 博客平台、Citrix 虚拟化产品等被披露存在多个安全漏洞，对企业信息化应用安全构成威胁。而 7-Technologies 公司 Interactive Graphical SCADA System 和亚控公司 Kingview 等工业控制系统软件存在综合评级为“高危”的安全漏洞，使得相关行业生产运行安全受到威胁。

CNVD 提醒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

CNVD 整理和发布以下重要安全修补信息。

1、IBM 发布升级程序，修补 Lotus Domino 安全漏洞

本周，IBM 发布升级程序，修补了 Lotus Domino 的安全漏洞。IBM Lotus Domino 服务器是一款基于 WEB 合作的应用程序架构。利用上述产品漏洞，远程攻击者可以提交特制端报文使 Lotus Domino 服务器崩溃。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/sites/main/preview/bdgg_preview.htm?tid=6471

2、北京亚控科技发布修复信息，修复 SCADA 程序堆缓冲区溢出漏洞

本周，国内工业控制系统生产厂商——北京亚控科技发布安全公告，发布了 kingview 组态王相关产品 HistoryServer.exe 漏洞补丁，修复了其中的缓冲区溢出漏洞，对于将信息数据库放在互联网上运行并开放 777 端口的 KingView 组态王产品需进行更新。

更新步骤：首先停止 KingView 的历史服务 HistorySvr 的运行，再将补丁文件 nettransdll.dll 直接拷贝覆盖 KingView 安装目录下的 nettransdll.dll，最后重新启动历史服务 HistorySvr 运行。

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。



本周要闻速递

1. 多款安卓手机管理软件存 WiFi 漏洞

近日，豌豆荚、腾讯手机助手等多款 Android 手机管理软件曝出安全漏洞，在公共 WiFi 环境下，Android 手机用户可能会被攻击者盗取所有个人隐私信息，危及数千万用户。有分析认为，这是目前为止国内最严重的智能手机安全风险，需提醒广大 Android 用户尽快升级软件程序修复漏洞。安全专家介绍，这类软件主要通过 FTP 服务来管理手机文件，但如果技术实现存在漏洞，就会导致在同一网络下的计算设备均能够登录 FTP 访问该手机。攻击者可恶意访问、上传、下载或篡改、删除手机信息，包括手机内存、存储卡中的照片、短信、聊天记录、电话录音、视频以及其他文档等个人隐私。

参考链接：<http://news.itxinwen.com/communication/inland/2011/1222/382257.html>

2. Mozilla 发布补丁更新，修复多个安全漏洞

Mozilla 修复了最新版本 Firefox9 浏览器软件中的 6 个安全漏洞，其中两个补丁修复了与 HTML5 有关的安全漏洞。Mozilla 在发布 Firefox9 之后不到一天就发布了一个软件更新。其中 4 个安全漏洞是“严重”等级的，其余的两个安全漏洞中，一个是“高”威胁等级的，另一个是“中等”威胁等级的。Mozilla 还在 12 月 21 日发布了一个补丁修复引起 Mac 版 Firefox 浏览器崩溃的瑕疵。Mozilla 还发布了 Firefox3.6.125 版，修复在 Mac OS X 版 Firefox 浏览器中的 Java .jar 安全漏洞。Mozilla 最近加快了开发周期，每 6 个星期进行一次网络浏览器升级。Firefox10 预计在 2012 年 1 月 31 日推出。

参考链接：<http://www.cnbeta.com/articles/166851.htm>

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