

信息安全漏洞周报

2011 年 11 月 21 日-2011 年 11 月 27 日

2011 年第 47 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 122 个，其中高危漏洞 42 个、中危漏洞 75 个、低危漏洞 5 个。上述漏洞中，可利用来实施远程攻击的漏洞有 109 个。本周收录的漏洞中，已有 84 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“Microsoft Windows Kernel 'Win32k.sys'键盘布局拒绝服务漏洞”等漏洞的零日攻击代码，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 5 家成员单位和多个合作伙伴报送了本周收录的全部 122 个漏洞，各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技、恒安嘉新、安天实验室的数量较多。此外，本周还收录了国网电力科学研究院信息安全网络安全实验室以及来自 CNVD 合作伙伴 WOORYUN 网站白帽子的 3 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	72	0
绿盟科技	61	0
恒安嘉新	46	0
安天实验室	30	0
安氏领信	1	0
国网电力科学研究院 信息网络安全实验室	1	1
乌云	2	2
总计	122（去重）	0

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Real Networks、Linux、WordPress、TYPO3 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	Real Networks	19	15.6%
2	Linux	12	9.8%
3	WordPress	7	5.7%
4	TYPO3	4	3.3%
5	One Click Orgs	4	3.3%
6	IBM	3	2.5%
7	FFmpeg	3	2.5%
8	Atlassian Software Systems	3	2.5%
9	Jenkins CI	2	1.6%
10	Microsoft	1	0.8%
11	其它	64	52.4%

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、Real Networks RealPlayer 安全漏洞

Real Networks RealPlayer 是一款多媒体播放程序。本周，RealPlayer 被披露存在多个安全漏洞，远程攻击者可以利用漏洞发起缓冲区溢出攻击、破坏内存或造成其他未明影响。CNVD 收录的相关漏洞包括：Real Networks RealPlayer 存在未明漏洞（CNVD-2011-08643、CNVD-2011-08640、CNVD-2011-08638、CNVD-2011-08635、CNVD-2011-08634、CNVD-2011-08632）、Real Networks RealPlayer 堆内存破坏漏洞（CNVD-2011-08641）、Real Networks RealPlayer 整数下溢漏洞（CNVD-2011-08639）。其中，“Real Networks RealPlayer 堆内存破坏漏洞（CNVD-2011-08641）”和“Real Networks RealPlayer 整数下溢漏洞（CNVD-2011-08639）”的综合评级为“高危”。目前，厂商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/vulnerability/CNVD-2011-08643>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08641>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08640>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08639>
<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08638>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08635>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08634>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08632>

2、Linux Kernel 安全漏洞

Linux Kernel 是开源操作系统 Linux 所使用的内核。本周，Linux 内核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执行任意代码、提升特权或发起拒绝服务攻击，使系统崩溃。CNVD 收录的相关漏洞包括：Linux Kernel 'hardlink'远程栈缓冲区溢出漏洞、Linux Kernel 'hardlink'远程整数溢出漏洞、Linux Kernel 未授权访问漏洞（CNVD-2011-08705）、Linux Kernel VLAN 报文处理远程拒绝服务漏洞、Linux Kernel 'hfs_mac2asc()'本地特权提升漏洞、Linux Kernel Headroom 检查'udp6_ufo_fragment()'远程拒绝服务漏洞、Linux Kernel 空指针引用拒绝服务漏洞、Linux Kernel 'IFF_TX_SKB_SHARING'本地拒绝服务漏洞。其中，“Linux Kernel Headroom 检查'udp6_ufo_fragment()'远程拒绝服务漏洞”的综合评级为“高危”。目前，厂商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/vulnerability/CNVD-2011-08710>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08708>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08705>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08657>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08642>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08637>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08636>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08633>

3、FFmpeg 产品安全漏洞

FFmpeg 是一款用于录制、转换和流化音频和视频的完整解决方案。本周，FFmpeg 产品存在多个可被远程利用的安全漏洞。攻击者可以利用漏洞发起缓冲区溢出攻击，导致系统拒绝服务。CNVD 收录的相关漏洞包括：FFmpeg 越界读漏洞、FFmpeg 'vp3_dequant()' 函数缓冲区溢出漏洞、FFmpeg QDM2 缓冲区溢出漏洞。上述漏洞的综合评级均为“高危”。目前，FFmpeg 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/vulnerability/CNVD-2011-08662>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08661>

<http://www.cnvd.org.cn/vulnerability/CNVD-2011-08659>

4、Microsoft Windows Kernel 'Win32k.sys'键盘布局拒绝服务漏洞

Microsoft Windows 是微软公司的操作系统产品。本周，Windows 内核被披露存在一个本地拒绝服务漏洞。由于系统在装载键盘布局文件时，win32k.sys 驱动存在一个索引错误，本地攻击者可以利用该漏洞发起拒绝服务攻击，使系统崩溃。目前，互联网上

已经出现针对该漏洞的攻击代码，主要影响 Microsoft Windows XP 家庭版和专业版。微软尚未发布该漏洞的补丁程序，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/vulnerability/CNVD-2011-08663>

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/vulnerability/advancedSearch>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2011-08719	CMS Balitbang 'hal'参数存在多个 SQL 注入漏洞	高	暂无
CNVD-2011-08716	ZABBIX 'only_hostid'参数 SQL 注入漏洞	高	ZABBIX 1.8.9 已修复此漏洞，建议用户下载使用： http://www.zabbix.com/index.php
CNVD-2011-08711	Novell Netware 'XNFS.NLM'组件 'xdrDecodeString()'远程缓冲区溢出漏洞	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://download.novell.com/Download?buildid=Cfw1tDezgbw~
CNVD-2011-08693	Dolibarr SQL 注入漏洞	高	用户可联系供应商获得补丁信息： http://www.dolibarr.org/
CNVD-2011-08687	Pro Clan Manager SQL 注入漏洞	高	暂无
CNVD-2011-08684	PHP-Nuke URI SQL 注入漏洞	高	暂无
CNVD-2011-08683	PmWiki 'PageListSort()'函数 PHP 代码注入漏洞	高	PmWiki 2.2.35 已经修复此漏洞，建议用户下载使用： http://www.pmichaud.com/wiki/PmWiki/PmWiki
CNVD-2011-08680	Hastymail 'rs'和'rsargs[]'参数远程代码注入漏洞	高	暂无
CNVD-2011-08681	Namazu 'uri'字段基于栈的缓冲区溢出漏洞	高	Namazu Project Namazu 2.0.21 和 2.0.20 已经修复此漏洞，建议用户下载使用： http://www.namazu.org/
CNVD-2011-08672	GOCDKEY 推广系统上传漏洞	高	GOCDKEY 未能提供漏洞补丁，建议采用以下临时措施： 取消网站图片 uploadfile 目录的脚本执行权限； 建议将服务器组件由 IIS 6 升级至 IIS 7。

表 3 部分高危漏洞列表

小结：本周，Real Networks 发布安全更新，修复了 RealPlayer 播放器存在的多个安全漏洞。远程攻击者可以利用漏洞发起缓冲区溢出攻击、破坏内存或造成其他未明影响。同时，Linux Kernel 和 FFmpeg 产品也被披露存在多个漏洞。Microsoft Windows 和 QQ Player 零日漏洞对广大用户构成较大威胁。

此外，CNVD 本周收录了多个在国内外网站信息系统中广泛应用的 web 应用程序存在的 SQL 注入、文件上传等漏洞，利用这些漏洞有可能获得网站数据库后台敏感信息甚至是操作系统管理权限。目前，互联网上已经出现针对上述漏洞的攻击测试实例。

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

CNVD 整理和发布以下重要安全修补信息。

1、IBM 发布升级程序，修补多款产品安全漏洞

本周，IBM 发布升级程序，修补了 Lotus Mobile Connect、WebSphere Application Server 等多款产品存在的安全漏洞。攻击者可以利用漏洞获得敏感信息或劫持用户会话。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/5995>

<http://www.cnvd.org.cn/patch/5956>

<http://www.cnvd.org.cn/patch/6027>

本周要闻速递

1. 搜狗浏览器被披露存在安全漏洞

11 月 22 日，据国外知名技术网站爆料称，搜狗浏览器存在严重的安全漏洞。黑客可以利用漏洞控制装有搜狗浏览器的任何电脑，专家认为，这将严重威胁用户的财产和隐私安全。11 月 14 日，网友在国外知名的技术网站爆料称，搜狗浏览器很容易受到“缓冲区溢出漏洞”攻击，影响搜狗浏览器官方版本和之前的版本。也就是说，黑客很有可能利用该漏洞在搜狗用户电脑上运行任意代码，包括以管理员权限植入病毒并控制系统。事实上，根据贴出的演示图片显示，搜狗浏览器在打开一个网页时，电脑中的计算器被调用出来。业内专家表示，如果黑客将调用计算器的程序换成病毒，那么搜狗浏览器用户将面临严重风险。

参考链接：http://www.kejixun.com/a/2011-11-22/10126_1.html

2. iCloud 恢复备份出现安全漏洞

iCloud 为 iOS5 用户带来诸多方便，他们终于可以抛弃数据线，无线备份和恢复设备。然而，将自己的内容传输到苹果服务器，不见得非常安全。最近有用户发现了 iCloud 一个严重的问题，可导致用户邮箱地址的泄露。浏览苹果官网的讨论区发现，苹果实际上已经注意到这个安全漏洞，但在最新的 iOS5 更新中并未解决该问题。希望苹果能在下一次更新中解决这么一个严重的安全漏洞。

参考链接：<http://tech.163.com/11/1124/10/7JKBC HH0000915BE.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