

信息安全漏洞周报

2011 年 12 月 12 日-2011 年 12 月 18 日

2011 年第 50 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 115 个，其中高危漏洞 32 个、中危漏洞 79 个、低危漏洞 4 个。上述漏洞中，可利用来实施远程攻击的漏洞有 101 个。本周收录的漏洞中，已有 75 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“ConfigServer Firewall 缓冲区溢出漏洞”、“DoceboLMS 'message[attach]'任意文件上传漏洞”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 4 家成员单位和 1 家单位报送了本周收录的全部 115 个漏洞。其中，北京网御星云信息技术有限公司报送了某款在学校中应用较广泛的网站管理系统（CMS）存在的 SQL 注入漏洞，属原创漏洞。目前，CNVD 已经协调软件厂商进行处置。

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	87	0
绿盟科技	78	0
安天实验室	34	0
恒安嘉新	24	0
北京网御星云信息技术有限公司	1	1
总计	115（去重）	1

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、Google、IBM 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	Microsoft	20	17.4%
2	Google	16	13.9%
3	IBM	4	3.5%
4	RSA Security	3	2.6%
5	Winamp	3	2.6%
6	Adobe	2	1.7%
7	Mozilla	2	1.7%
8	Wordpress	2	1.7%
9	Nagios	2	1.7%
10	Browser CRM	2	1.7%
11	其它	59	51.5%

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、ConfigServer Firewall 缓冲区溢出漏洞

ConfigServer Firewall 是一款防火墙软件。本周，ConfigServer Firewall 被披露存在一个缓冲区溢出漏洞。由于应用程序未能正确处理用户提交的输入，远程攻击者可以利用漏洞发起缓冲区溢出攻击，造成应用程序崩溃或任意代码执行。该漏洞的综合评级为“高危”。目前，互联网上已经出现针对该漏洞的攻击代码，且厂商尚未发布漏洞的补丁程序，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/sites/main/preview/ldgg_preview.htm?tid=35420

2、Microsoft 产品安全漏洞

本周，微软发布了 2011 年 12 月份的月度例行安全公告，共包含 13 项安全更新。此次更新修复了涉及 Windows 操作系统和组件、Office 办公套件和软件、IE 浏览器等多款产品存在的 19 个安全漏洞。利用上述漏洞，攻击者可以远程执行代码、窃取敏感信息，或本地提升特权。CNVD 收录的相关漏洞包括：Microsoft Publisher 远程内存破坏漏洞、Microsoft Publisher 非法指针远程代码执行漏洞、Microsoft Publisher 数组索引越界远程代码执行漏洞、Microsoft Windows OLE 属性远程代码执行漏洞（CNVD-2011-09002）、Microsoft Internet Explorer 跨域信息泄露漏洞（CNVD-2011-08992）、Microsoft Internet Explorer XSS 过滤器跨域信息泄露漏洞、Microsoft Excel 远程代码执行漏

洞（CNVD-2011-08991）、Microsoft Windows Time 组件远程代码执行漏洞等。其中，“Microsoft Windows Time 组件远程代码执行漏洞”的综合评级为“高危”。值得注意的是，此前曾被 Duqu 病毒(“超级工厂”Ⅱ代)利用的 Windows 内核高危漏洞（CNVD-2011-08292），也在本次发布的安全更新中得到微软官方修复。由于 Duqu 病毒发起攻击的目标为工业控制领域的信息系统，CNVD 提醒工控系统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=35499
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35501
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35503
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35504
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35494
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35496
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35493
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35505

3、Google Chrome 产品安全漏洞

Google Chrome 是一款 WEB 浏览器。本周，Google 修复了 Chrome 存在的多个安全漏洞，避免攻击者可以利用漏洞进行伪造攻击，窃取敏感信息或执行任意代码。CNVD 收录的相关漏洞包括：Google Chrome 内存错误引用漏洞（CNVD-2011-09033、CNVD-2011-09034、CNVD-2011-09041）、Google Chrome 越界写漏洞（CNVD-2011-09035）、Google Chrome 缓冲区溢出漏洞（CNVD-2011-09037、CNVD-2011-09039）、Google Chrome 越界读漏洞（CNVD-2011-09038）、Google Chrome 破坏内存漏洞（CNVD-2011-09028）。除“Google Chrome 越界读漏洞（CNVD-2011-09038）”之外的漏洞综合评级均为“高危”。CNVD 提醒 Google Chrome 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=35539
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35540
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35541
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35543
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35544
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35546
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35548
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35534

4、IBM AIX 产品安全漏洞

IBM AIX(Advanced Interactive eXecutive)是 IBM 公司开发的一套类 UNIX 操作系统。本周，IBM AIX 被披露存在的多个安全漏洞。攻击者可以利用漏洞进行未授权操

作或造成其他未明影响。CNVD 收录的相关漏洞包括：IBM AIX 存在未明漏洞、IBM AIX Inventory Scout 代码符号链接漏洞、IBM AIX Inventory Scout 任意文件删除漏洞。除“IBM AIX Inventory Scout 任意文件删除漏洞”外，IBM 已发布其余漏洞的修补程序，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=35535
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35537

5、Adobe ColdFusion 安全漏洞

Adobe ColdFusion 是一款动态 Web 内容服务器。本周，上述 Adobe 产品被披露存在两个跨站脚本漏洞，攻击者可以利用漏洞构建恶意链接，诱使用户解析，进而窃取敏感信息或劫持用户会话。CNVD 收录的相关漏洞包括：Adobe ColdFusion 'cfform' 标签跨站脚本漏洞（CNVD-2011-08987）、Adobe ColdFusion RDS 跨站脚本漏洞（CNVD-2011-08986）。目前，厂商已经发布了上述漏洞的补丁程序，CNVD 提醒 Adobe 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=35488
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=35489

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。参考链接如下所示：

<http://www.cnvd.org.cn/sites/main/twaindex/advancedSearch.htm?columnid=52>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2011-09017	Yahoo! CD Player ActiveX Control 'open()'方法栈缓冲区溢出漏洞	高	暂无
CNVD-2011-08978	WordPress 插件 UPM Polls 'PID' SQL 注入漏洞	高	暂无
CNVD-2011-08962	Linux Kernel Network Namespace 远程拒绝服务漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://www.kernel.org/
CNVD-2011-08976	Winamp 整数溢出漏洞（CNVD-2011-08976）	高	NullSoft Winamp 5.623 已经修复此漏洞，建议用户下载使用： http://forums.winamp.com/showthread.php?t=332010
CNVD-2011-08950	HTC Touch2 T3333 HTCVideoPlayer 内存破坏漏洞	高	暂无
CNVD-2011-08969	XOOPS 'selgroups'参数 SQL 注入漏洞	高	暂无

CNVD-2011-08959	Pipemail 'bat_socket_read'函数内存破坏漏洞	高	暂无
CNVD-2011-09058	Seotoaster 'selectUserIdByLoginPass()' SQL注入漏洞	高	厂商已经发布了 Seotoaster 1.9 更新版本，建议用户下载使用： http://www.seotoaster.com/
CNVD-2011-09013	Sterling Trader 远程栈溢出漏洞	高	暂无
CNVD-2011-08981	多个 SepCity 产品存在未明 SQL 注入漏洞	高	用户可联系供应商获得补丁信息： http://www.sepcity.com/

表 3 部分高危漏洞列表

小结：本周，Microsoft 发布了 2011 年 12 月份的月度例行安全公告，修复了涉及 Windows 操作系统和组件、Office 办公套件和软件、IE 浏览器等多款产品存在的多个安全漏洞。其中包含此前曾被 Duqu 病毒(“超级工厂” II 代)利用的 Windows 内核高危漏洞（CNVD-2011-08292）。CNVD 提醒工业控制领域的相关用户尽快下载补丁更新。

本周 CNVD 还收录了 Google Chrome 浏览器、Wordpress 插件、Yahoo! CD Player、Winamp 媒体播放器等应用广泛的应用软件以及 IBMAIX 和 Linux 等多个操作系统的漏洞，上述漏洞综合评级多为“高危”和“中危”。

另外，ConfigServer Firewall 防火墙软件的零日漏洞也对广大用户也构成较大威胁，请使用上述产品的网站服务器管理员、个人用户注意防范。

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、Linux 发布升级程序，修补 Kernel 安全漏洞

Linux Kernel 是开源操作系统 Linux 所使用的内核。本周，Linux 发布升级程序，修补了 Kernel 的安全漏洞，避免远程攻击者利用漏洞进行拒绝服务攻击。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=6252



本周要闻速递

1. iOS 再爆 iMessage 安全漏洞

12月16日消息，苹果的新操作系统 iOS 5 在继爆出电池漏洞之后，又出现了 iMessage 的安全漏洞。使用远程删除 iPhone 资料后的手机，在重新激活后会获得以前 iMessage 短信。安全专家表示，这可能是由于 iOS 5 存在漏洞造成，原来的 SIM 卡会重新激活 iMessage，而激活后 iMessage 信息存储在 iPhone 的某个文件中无法删除。

参考链接：<http://www.enet.com.cn/article/2011/1216/A20111216948787.shtml>

2. WP7.5 短信安全漏洞

据国外媒体报道，运行微软 Windows Phone 7.5 软件的设备容易受到拒绝服务攻击。这种攻击将关闭用户手机的短信功能。测试表明，这个安全漏洞影响到运行这个移动操作系统的各种设备。一个 Facebook 聊天消息和 Windows Live Messenger 消息也能够利用这个安全漏洞。到目前为止，这个消息中心安全漏洞的唯一解决方案是硬重启和删除设备数据。运行 Android 和 iOS 系统的设备也曾受到短信安全漏洞的影响。研究人员还发现一个短信实施安全漏洞。他们利用这个安全漏洞能够引起 Android 手机临时崩溃，阻止用户接听或者打电话以及发短信。苹果和谷歌已经修复了这些安全漏洞。微软代表没有立即对此消息发表评论。

参考链接：<http://finance.yynet.com/3.1/1112/14/6600299.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