

信息安全漏洞周报

2012 年 1 月 9 日-2012 年 1 月 15 日

2012 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 104 个，其中高危漏洞 43 个、中危漏洞 59 个、低危漏洞 2 个。上述漏洞中，可利用来实施远程攻击的漏洞有 95 个。本周收录的漏洞中，已有 67 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“TinyWebGallery 存在多个远程命令执行漏洞”、“GreenBrowser 搜索栏快捷按钮两次释放远程内存破坏漏洞”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 5 个成员单位报送了本周收录的全部 104 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、绿盟科技报送数量较多。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	71	0
绿盟科技	50	0
恒安嘉新	24	0
安天实验室	18	0
安氏领信	3	0
总计	104（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 Microsoft、HP、IBM、NTRglobal 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	7	6.7%

2	HP	6	5.7%
3	IBM	6	5.7%
4	NTRglobal	5	4.8%
5	Adobe	4	3.8%
6	ImpressCMS	4	3.8%
7	VMWare	4	3.8%
8	WordPress	3	2.9%
9	Wireshark	3	2.9%
10	Google	3	2.9%
11	其它	59	57%

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、IBM 产品安全漏洞

本周，IBM 的多款产品 Cognos TM1 Executive Viewer、Web Experience Factory、Telelogic/Rational License Server License Manager 等被披露存在多个安全漏洞。IBM Cognos TM1 Executive Viewer 经营决策程序是一款提供进阶分析和报表制作功能的产品；IBM Web Experience Factory 则用于开发跨桌面、移动设备和平板电脑的 Web 前端；IBM Telelogic/Rational License Server License Manager 是一款证书管理服务器。远程攻击者可以利用上述产品漏洞执行任意脚本代码、获得敏感信息、劫持用户会话或进行拒绝服务和跨站脚本攻击。CNVD 收录的相关漏洞包括：IBM HTTP Server 存在多个跨站脚本漏洞、IBM Telelogic/Rational License Server License Manager 日志文件上传漏洞、IBM WebSphere Application Server Community Edition Tomcat Container 拒绝服务漏洞、IBM Web Experience Factory 智能刷新 HTML 注入漏洞、IBM Cognos TM1 Executive Viewer 跨站脚本漏洞（CNVD-2012-09341、CNVD-2012-09340）。其中，“IBM Telelogic/Rational License Server License Manager 日志文件上传漏洞”的综合评级均为“高危”。目前，IBM 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=37099
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36910
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36909
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37230
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37131

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37097

2、Microsoft 产品安全漏洞

本周，微软发布了 2012 年 1 月份的月度例行安全公告，包含 7 项安全更新，共修复了涉及 Windows 操作系统和组件以及 Microsoft 防跨站点脚本库(AntiXSS)存在的 8 个安全漏洞。利用上述漏洞，攻击者可以远程执行代码、绕过安全验证、窃取敏感信息或本地提升特权。CNVD 收录的相关漏洞包括：Microsoft AntiXSS 库过滤模块安全绕过漏洞、Microsoft Windows ClickOnce 应用程序安装程序远程代码执行漏洞、Microsoft DirectX DirectShow 过滤器远程代码执行漏洞、Microsoft Windows CSRSS 本地特权提升漏洞、Microsoft Windows 内核 SafeSEH 安全绕过漏洞、Microsoft Windows Media Player 'winmm.dll' MIDI 文件解析远程代码执行漏洞、Microsoft Windows 对象包装程序远程代码执行漏洞。其中，“Microsoft DirectX DirectShow 过滤器远程代码执行漏洞”、“Microsoft WindowsMedia Player 'winmm.dll' MIDI 文件解析远程代码执行漏洞”的综合评级均为“高危”。CNVD 提醒 Microsoft 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=37048
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37068
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37091
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37089
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37095
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37096
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37098

3、Adobe 产品安全漏洞

Adobe Reader/Acrobat 是一款处理 PDF 文件的应用程序。本周，Adobe Reader/Acrobat 被披露存在多个内存破坏漏洞，攻击者可以利用漏洞以应用程序上下文执行任意代码。CNVD 收录的相关漏洞包括：Adobe Acrobat/Reader 堆破坏漏洞（CNVD-2012-09354、CNVD-2012-09357、CNVD-2012-09359、CNVD-2012-09355）。上述漏洞的综合评级均为“高危”。目前，Adobe 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=37028
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37049
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37088
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=37029

4、WordPress 插件安全漏洞

WordPress 是使用 PHP 语言开发的网页平台软件。本周，WordPress 多款插件存在多个安全漏洞。攻击者可以利用漏洞进行跨站脚本或 SQL 注入攻击。CNVD 收录的相关

漏洞包括：WordPress 插件 Pay With Tweet 跨站脚本漏洞、WordPress 插件 Pretty Link Lite 'slug'参数跨站脚本漏洞、WordPress 插件 Pay With Tweet SQL 注入漏洞。其中，“WordPress 插件 Pay With Tweet SQL 注入漏洞”的综合评级为“高危”。除“WordPress 插件 Pretty Link Lite 'slug'参数跨站脚本漏洞”外，互联网上均已经出现针对其余漏洞的攻击代码。目前，厂商尚未发布上述漏洞的补丁程序。CNVD 提醒广大 WordPress 用户随时关注厂商主页，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=36808
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36768
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=36788

5、TinyWebGallery 存在多个远程命令执行漏洞

TinyWebGallery 是一款采用 PHP 开发的免费网络相册程序。本周，TinyWebGallery 被披露存在多个远程命令执行漏洞。由于程序中包含的'inc/filefunctions.inc.php'和'info.php'脚本未能正确过滤用户提交的输入，攻击者可以利用漏洞以 WEB 权限执行任意 SHELL 命令。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，主要影响 TinyWebGallery 1.8.3 版本。厂商尚未发布该漏洞的修补程序，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=36868

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-2012-09402	HP StorageWorks 默认账户漏洞	高	暂无
CNVD-2012-09324	IpTools Tiny TCP/IP 服务器目录遍历漏洞	高	暂无
CNVD-2012-09382	NTR ActiveX 控件缓冲区溢出漏洞（CNVD-2012-09382）	高	NTRglobal NTR ActiveX control 2.0.4.8 已经修复此漏洞，建议用户下载使用： http://www.ntrglobal.com/
CNVD-2012-09383	NTR ActiveX 控件任意函数指针漏洞	高	NTRglobal NTR ActiveX control 2.0.4.8 已经修复此漏洞，建议用户下载使用： http://www.ntrglobal.com/
CNVD-2012-09389	TFTP Server 读请求远程缓冲区溢出漏洞	高	暂无
CNVD-2012-09393	Wireshark 缓冲区溢出漏洞	高	Wireshark 1.6.5 和 1.4.11 已经修复此漏洞，建议用户下载使用： http://www.wireshark.org/

CNVD-2012-09381	Linux Kernel 远程拒绝服务漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息: https://bugzilla.redhat.com/show_bug.cgi?id=757143
CNVD-2012-09377	ExpressView 浏览器插件远程代码执行漏洞	高	暂无
CNVD-2012-09374	SumatraPDF 'fz_crash_abort()'任意空字节写漏洞	高	暂无
CNVD-2012-09342	HP LaserJet P3015 存在未明安全绕过漏洞	高	HP LaserJet P3015 07.080.3 固件版本已修复此漏洞, 建议用户下载使用: http://h10010.www1.hp.com/wwpc/sg/en/sm/WF06b/18972-18972-3328059-236263-236263-3815797-3815800.html

表 3 部分高危漏洞列表

小结: 本周需要重点关注微软发布的 2012 年 1 月份月度例行安全公告, 其中包含 7 项安全更新, 共修复了涉及 Windows 操作系统和组件以及 Microsoft 防跨站点脚本库(AntiXSS)存在的 8 个安全漏洞。这些修复措施可防范攻击者发起的远程执行代码、绕过安全验证、窃取敏感信息或本地提升特权等攻击。本周, Wordpress 插件、IBM、Adobe 和 TinyWebGallery 的应用产品被披露存在多个安全漏洞, 远程攻击者可以利用漏洞执行任意脚本代码、获得敏感信息、劫持用户会话或进行拒绝服务、跨站脚本等攻击, 对企业和个人用户构成威胁。

此外, 本周出现的 HP StorageWorks 默认账户漏洞和 Linux Kernel 远程拒绝服务漏洞也对企业级和个人桌面用户服务器或主机构成安全威胁。

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、Linux 发布升级程序, 修补内核多个安全漏洞

本周, Linux 发布升级程序, 修补了 Kernel 多个安全漏洞。远程攻击者可以利用漏洞破坏内存或进行拒绝服务攻击。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=7351

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=7411

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=7352

本周要闻速递

1. 微软发布 2012 年首批安全补丁 修复多个漏洞

微软刚刚发布了今年首批安全补丁，1 月份共更新 7 个补丁，修复了 Windows 操作系统和其他软件中的 8 个安全漏洞。微软本次修复多个可能造成信息泄露的漏洞，此类补丁在去年很少更新，可见微软也加强了网络信息安全的防范。据悉，微软本次修复了包括 Windows 7 和 Windows Server 2008 R2 在内的所有版本的 Windows 中的安全漏洞。在这 7 个补丁中只有 1 个是“严重”等级的，其余的都是“重要”等级的补丁。这个“严重”等级的补丁修复媒体播放器软件中的一个远程执行代码漏洞。值得注意的是，微软本次修复了包括 SSL/TLS 和 AntiXSS 库中可能允许信息泄露的多个安全漏洞。恶意攻击者可利用上述漏洞截获网络传输中的加密的信息，甚至一些受到影响的网站中的信息。也就是说，微软本次修复的漏洞可能影响普通上网网民和一些网站。

参考链接: <http://news.csdn.net/a/20120111/310477.html>

2. A5 越狱将临 iOS 5.1 Beta3 已修复越狱漏洞

日前，美国越狱小组 Pwnage 团队的成员 nadeem97 在推特上表示，苹果在最新发布 iOS 5.1 Beta 3 更新中已经修补了 Corona iOS 5.0.1 完美越狱所利用的漏洞，建议用户尽快升级更新至 iOS 5.0.1。而从目前的情况来看，苹果可能即将发布 iOS 5.1 正式版。而此前 Pod2g 也已经在博客上表示 A5 完美越狱工作目前已经处于最后的阶段，计划越狱 iPhone 4S 以及 iPad 2 的用户应该在苹果还认证之前尽快更新到 iOS 5.0.1，一旦苹果发布 iOS 5.1 之后用户就无法更新了。

参考链接: <http://mobile.pconline.com.cn/dclub/1201/2652802.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