

信息安全漏洞周报

2012 年 4 月 2 日-2012 年 4 月 8 日

2012 年第 14 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 113 个，其中高危漏洞 50 个、中危漏洞 62 个、低危漏洞 1 个。上述漏洞中，可利用来实施远程攻击的漏洞有 106 个。本周收录的漏洞中，已有 73 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“MailMax 'USER' POP3 命令远程缓冲区溢出漏洞”、“MyBB 'index.php' SQL 注入漏洞”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 7 家成员单位和多个合作伙伴报送了本周收录的全部 113 个漏洞。各单位报送情况如表 1 所示。其中，绿盟科技、启明星辰、安天实验室、天融信等单位报送数量较多。国内漏洞研究者（个人报送者）向 CNVD 报送了 5 起涉及政府和重要信息系统部门的漏洞事件。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	93	0
绿盟科技	37	0
天融信	55	0
安天实验室	20	0
恒安嘉新	12	0
东软	4	0
安氏领信	5	1
上海交通大学	1	1
个人上报者	3	3

报送总计	230	5
总计	113（去重）	5

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Google、HP、ImageMagick、ArticleSetup、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	Google	13	11.5%
2	HP	5	4.4%
3	ImageMagick	4	3.5%
4	ArticleSetup	4	3.5%
5	Invensys	3	2.7%
6	Csound	3	2.7%
7	IBM	3	2.7%
8	RedHat	3	2.7%
9	Adobe	2	1.8%
10	Quest	2	1.8%
11	其它	71	62.7%

表 2 漏洞产品涉及厂商分布统计表



漏洞按影响类型统计

本周，CNVD 收录了 113 个漏洞。其中操作系统漏洞 1 个，应用程序漏洞 76 个，WEB 应用漏洞 27 个，网络设备漏洞 4 个，数据库漏洞 1 个，安全产品漏洞 4 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	1
应用程序漏洞	76
WEB 应用漏洞	27
网络设备漏洞	4
数据库漏洞	1
安全产品漏洞	4

表 3 漏洞按影响类型统计表

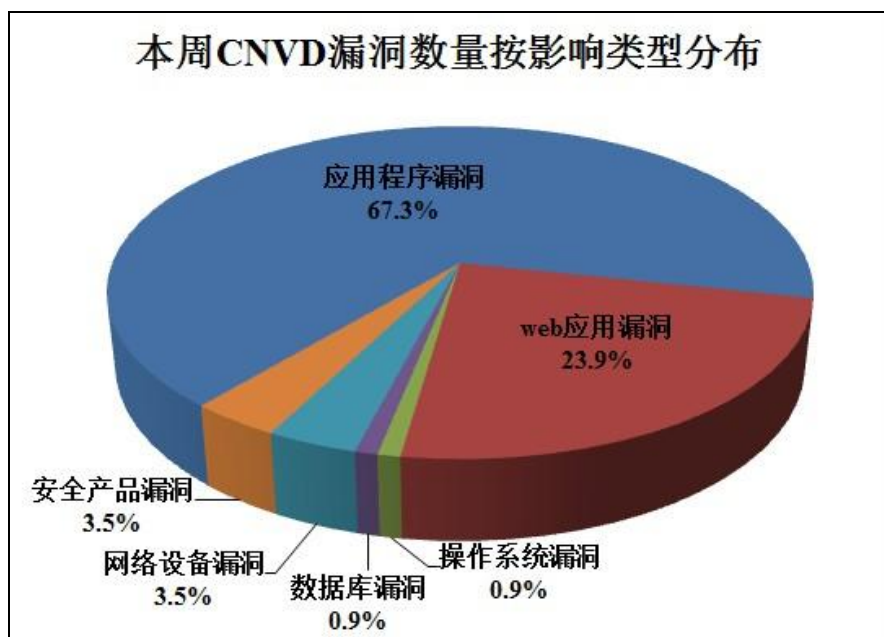


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 共收录了 4 个网络设备漏洞。其中，CNVD 成员单位安氏领信公司报送某国产无线网络控制器权限绕过漏洞已经处置完毕，正式收录。此外，CNVD 还收录了“NetGear ProSafe Wireless-N 8-port Gigabit VPN Firewall FVS318N 路由器安全绕过漏洞”、“TP-Link 8840T DSL 路由器安全绕过漏洞”和“Sony Bravia 'hping'命令远程拒绝服务漏洞”，这些漏洞的综合评级均为“中危”。目前，互联网上已经出现针对“某无线网络控制器权限绕过漏洞”和“Sony Bravia 'hping'命令远程拒绝服务漏洞”的攻击代码。

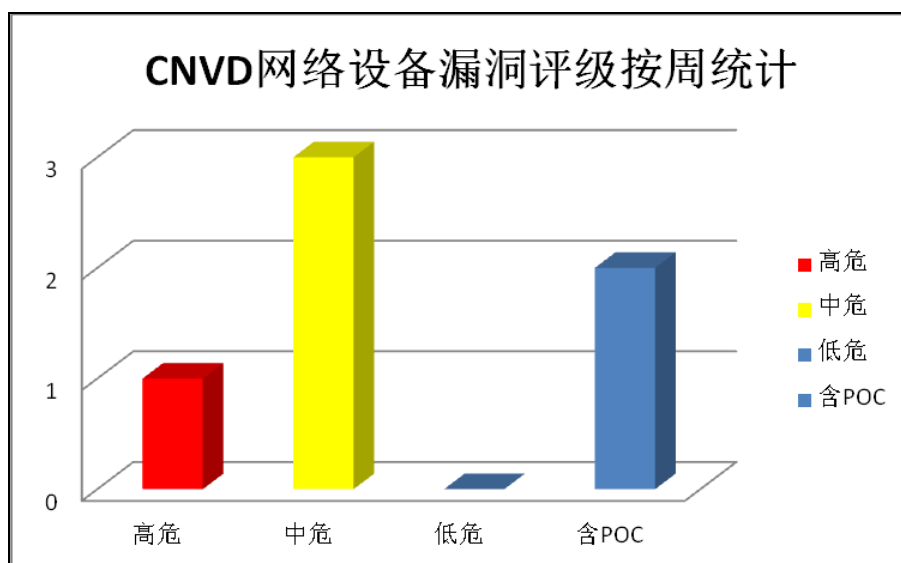


图 2 网络设备漏洞统计



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、Google Chrome 安全漏洞

Google Chrome 是一款 WEB 浏览器。本周，Google Chrome 被披露存在多个安全漏洞，攻击者可以利用漏洞构建恶意 URL，诱使用户解析，进而执行任意代码。CNVD 收录的相关漏洞包括：Google Chrome 脚本绑定内存错误引用漏洞、Google Chrome Focus 处理内存错误引用漏洞、Google Chrome 应用 style 命令漏洞、Google Chrome 媒体处理内存错误引用漏洞、Google Chrome HTMLMediaElement 内存错误引用漏洞、Google Chrome run-in 处理内存错误引用漏洞、Google Chrome box 处理内存错误引用漏洞、Google Chrome SVG 资源处理内存错误引用漏洞。上述漏洞的综合评级均为“高危”。目前，厂商已经发布这些漏洞的修补程序，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=46837
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46836
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46819
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46817
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46810
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46804
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46807
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46815

2、HP 产品安全漏洞

HP Business Availability Center(惠普业务可用性中心)是一款业务管理解决方案；HP Onboard Administrator 是一款机箱控制器软件；HP-UX（全称为 Hewlett Packard Unix）是一款用于惠普公司服务器产品的操作系统。本周，上述 HP 产品被披露存在多个漏洞，未经授权的远程攻击者可以利用漏洞构建恶意 URL，诱使用户解析，获得敏感信息、劫持用户会话，重定向用户到任意网站或进行拒绝服务攻击。CNVD 收录的相关漏洞包括：HP Business Availability Center 跨站脚本漏洞（CNVD-2012-11054）、HP Onboard Administrator 存在未明授权访问漏洞、HP Onboard Administrator 存在未明信息泄露漏洞、HP Onboard Administrator URL 重定向漏洞、HP-UX DCE 存在未明远程拒绝服务漏洞。其中，“HP Onboard Administrator 存在未明授权访问漏洞”和“HP-UX DCE 存在未明远程拒绝服务漏洞”的综合评级均为“高危”。目前，厂商已经发布这些漏洞的修补程序，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=46758

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46718

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46720

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46721

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46723

3、ImageMagick 安全漏洞

ImageMagick 是一款图像处理软件。本周，ImageMagick 被披露存在多个安全漏洞，攻击者可以利用漏洞发起拒绝服务攻击。CNVD 收录的相关漏洞包括：ImageMagick 拒绝服务漏洞（CNVD-2012-11100、CNVD-2012-11099、CNVD-2012-11098、CNVD-2012-11097）。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/sites/main/preview/ldgg_preview.htm?tid=46840

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46839

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46842

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46841

4、IBM 产品安全漏洞

IBM Cognos TM1 是一款业务分析软件，用于有效管理财务数据 IBM Tivoli Directory Server 是提供轻量级目录访问协议（LDAP）基础设施的解决方案；IBM Event Pump 主要用于搜索主机系统的事件信息。本周，上述 IBM 产品被披露存在多个漏洞，攻击者可以利用漏洞构建恶意 URL，诱使用户解析，获得敏感信息或劫持用户会话。CNVD 收录的相关漏洞包括：IBM Cognos TM1 Admin 服务器远程缓冲区溢出漏洞、IBM Tivoli Directory Server Web 管理工具跨站脚本漏洞、IBM Event Pump for z/OS 密码泄露漏洞。其中，“IBM Cognos TM1 Admin 服务器远程缓冲区溢出漏洞”的综合评级为“高危”。目前，厂商已经发布这些漏洞的修补程序，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=46751

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46753

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=46759

5、MailMax 'USER' POP3 命令远程缓冲区溢出漏洞

MailMax 是一款多线程邮件服务器软件。本周，MailMax 被披露存在一个缓冲区溢出漏洞。由于 MailMax POP3 服务未能正确处理"USER"请求，远程攻击者可以利用漏洞提交畸形请求，触发缓冲区溢出，执行任意代码。目前，互联网上已经出现针对该漏洞的攻击代码，主要影响 MailMax 4.6 版本。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=46775

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-2012-11019	ArticleSetup 'cat'参数 SQL 注入漏洞	高	暂无
CNVD-2012-11022	PHP Designer 2007-Personal 存在多个 SQL 注入漏洞	高	供应商发布了安全公告及相关补丁信息, 修复了此漏洞, 建议用户下载使用。避免攻击者可以利用这个问题在受影响的机器上执行任意代码, 达到攻击的目的: http://download.cnet.com/PHP-Designer-2007-Personal/3000-10248_4-10575026.html
CNVD-2012-10993	F5 FirePass SQL 注入漏洞	高	供应商发布了安全公告及相关补丁信息, 修复了此漏洞, 建议用户下载使用。避免成功利用后可允许未验证的攻击者控制应用、访问或修改数据: http://support.f5.com/kb/en-us/solutions/public/13000/400/sol13463.html
CNVD-2012-10991	Havalite CMS SQL 注入漏洞	高	暂无
CNVD-2012-11001	多个 Invensys 产品远程堆缓冲区溢出漏洞 (CNVD-2012-11001)	高	供应商发布了安全公告及相关补丁信息, 修复了此漏洞, 建议用户下载使用。避免攻击者可以利用漏洞以应用程序上下文执行任意代码: https://wdnresource.wonderware.com/support/docs/_SecurityBulletins/Security_Bulletin_LFSEC00000071.pdf
CNVD-2012-10999	libpng 'png_set_text_2()'函数内存破坏漏洞	高	供应商发布了安全公告及相关补丁信息, 修复了此漏洞, 建议用户下载使用。避免攻击者可以利用漏洞以应用程序上下文执行任意代码: http://www.libpng.org/pub/png/libpng.html
CNVD-2012-10994	Intuit QuickBooks 'HelpAsyncPluggableProtocol.dll'堆缓冲区溢出漏洞	高	暂无
CNVD-2012-11052	Hotel Booking Portal 'country'参数 SQL 注入漏洞	高	暂无
CNVD-2012-11045	Csound 'main()'整数溢出漏洞	高	供应商发布了安全公告及相关补丁信息, 修复了此漏洞, 建议用户下载使用。避免允许攻击者以应用程序上下文执行任意代码: http://csound.sourceforge.net/

CNVD-2012-11023	Ghostscript 'OutputFile'参数堆缓冲区溢出漏洞	高	供应商发布了安全公告及相关补丁信息，修复了此漏洞，建议用户下载使用。避免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： http://bugs.ghostscript.com/show_bug.cgi?id=692856
-----------------	------------------------------------	---	--

表 3 部分高危漏洞列表

小结：本周，Google Chrome 浏览器以及 HP 和 IBM 的多款产品被批露存在漏洞，未授权的攻击者可以利用漏洞窃取敏感企业以及用户的私密数据或执行任意代码。ImageMagick 软件也被批露存在多个漏洞。上述产品由于采用的企业和个人用户较多，需引起重视，加强防范。此外，MailMax 存在的零日漏洞在互联网上出现了攻击代码，也需引起相关用户的关注。

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、RedHat 发布升级程序，修补 RPM Package Manager 安全漏洞

本周，RedHat 发布升级程序，修补了 RPM Package Manager 存在的安全漏洞。攻击者可以利用漏洞构建恶意 RPM 文件，诱使用户读取，导致 RPM 崩溃，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/sites/main/preview/bdgg_preview.htm?tid=15235

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=15236

http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=15234

本周要闻速递

1. 苹果发布基于 Java 的木马漏洞补丁

据报道，Mac 电脑遭遇新变种的基于 Java 的木马攻击，该漏洞无需管理员密码即可自行安装木马程序到 OS X 系统。针对此漏洞，苹果迅速发布 Java for OS X Lion 2012-001 和 Java for Mac OS X 10.6 Update 7。此次更新针对 Mac OS X 10.6.8 Snow Leopard 和 10.7.3 Lion(包括 OS X 的 Server 版)，修复了 Java 10.6.0_29 的多个漏洞，包括当用户访问网站时，恶意代码会自行在 Mac 运行的漏洞；也包括新变种 Mac Flashback 木马漏洞。

参考链接：<http://security.ctocio.com.cn/446/12304946.shtml>

2. 多家返利网站或有漏洞

记者获悉，国内流行的“多多返利”建站系统存在高危漏洞，可能使黑客获得返利网站后台的超级管理员权限，并篡改、盗取网购用户的数据。保守估计，受该漏洞影响的网购人群多达数百万。昨天，记者登录“多多返利”官网看到，信息显示，QQ 返利网、51 返利网、丐网天猫等 20 多家国内知名的返利网站均使用了“多多返利”建站系统。有关负责人表示，一旦建站系统出现漏洞，其危害远远高于单独某个网站的漏洞，因为所有使用该系统的网站都将面临黑客入侵的风险。负责人表示，已将漏洞修复方案通知“多多返利”官方，建议各返利网站尽快下载使用其最新版本。

参考链接：http://news.dayoo.com/finance/201204/03/54401_108005614.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