

信息安全漏洞周报

2012 年 4 月 23 日-2012 年 4 月 29 日

2012 年第 17 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 134 个，其中高危漏洞 36 个、中危漏洞 91 个、低危漏洞 7 个。上述漏洞中，可利用来实施远程攻击的漏洞有 127 个。本周收录的漏洞中，已有 70 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“Samsung NET-i ware 存在多个远程漏洞”、“PHP Volunteer Management 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 134 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、恒安嘉新、安天实验室、天融信等单位报送数量较多。此外，网御星云报送了 3 个原创漏洞，个人上报者报送了 5 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	81	0
恒安嘉新	46	0
安天实验室	35	0
天融信	18	0
安氏领信	4	0
东软	3	0
网御星云	3	3
个人上报者	5	5
报送总计	195	8
录入总计	134（去重）	8

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、IBM、Drupal、Asterisk、PHP 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	12	9%
2	IBM	11	8.2%
3	Drupal	6	4.5%
4	Piwigo	4	3%
5	Asterisk	3	2.2%
6	PHP	3	2.2%
7	Joomla!	3	2.2%
8	RubyGems	3	2.2%
9	Microsoft	2	1.4%
10	Hitachi	2	1.4%
11	其它	85	63.4%

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 134 个漏洞。其中操作系统漏洞 3 个，应用程序漏洞 76 个，WEB 应用漏洞 54 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
操作系统漏洞	3
应用程序漏洞	76
WEB 应用漏洞	54
网络设备漏洞	0
数据库漏洞	0
安全产品漏洞	1

表 3 漏洞按影响类型统计表

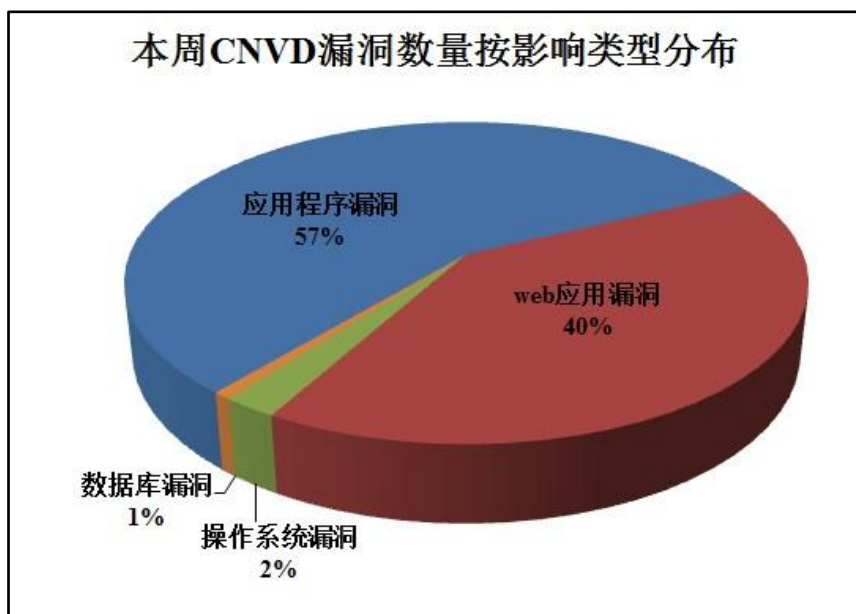


图 1 本周漏洞按影响类型分布

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、Mozilla 产品安全漏洞

4 月 24 日，Mozilla 发布了 14 项安全更新，修复了 Firefox、Thunderbird、SeaMonkey 中存在的 33 个安全漏洞。其中 7 项更新为“严重”级别，对应的漏洞均可被远程利用。利用上述漏洞，攻击者可以应用程序上下文执行任意代码、发起钓鱼攻击、窃取敏感信息或导致应用程序崩溃。其中，标号为 MFSA 2012-21 的更新修复了 19 个用于 Firefox 移动设备的 FreeType 字体库漏洞，攻击者可以利用这些漏洞破坏内存。

CNVD 收录的相关漏洞包括：Mozilla Firefox/Thunderbird/SeaMonkey IDBKeyRange 内存错误引用漏洞、Mozilla Firefox/Thunderbird/SeaMonkey 'cairo-dwrite'内存破坏漏洞（CNVD-2012-11491）、Mozilla Firefox/Thunderbird/SeaMonkey 内存破坏漏洞（CNVD-2012-11494、CNVD-2012-11495）、Mozilla Firefox/Thunderbird/SeaMonkey 堆缓冲区溢出漏洞（CNVD-2012-11498）、Mozilla Firefox/Thunderbird/SeaMonkey 拒绝服务漏洞（CNVD-2012-11506）、Mozilla Firefox/Thunderbird/SeaMonkey 跨站脚本漏洞（CNVD-2012-11504）、Mozilla Firefox/Thunderbird/SeaMonkey 站点身份欺骗漏洞等。

其中，除“Mozilla Firefox/Thunderbird/SeaMonkey 跨站脚本漏洞（CNVD-2012-11504）”和“Mozilla Firefox/Thunderbird/SeaMonkey 站点身份欺骗漏洞”外，其余漏洞的综合评级均为“高危”。CNVD 提醒广大 Mozilla 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=48096
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48082

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48083

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48079

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48086

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48094

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48092

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48078

2、IBM 产品安全漏洞

IBM Rational AppScan 是一款 Web 应用的安全测试工具；IBM Rational ClearQuest 是一款提供缺陷和变更跟踪、过程自动化、报表和生命周期追踪能力的软件错误追踪系统。本周，上述 IBM 产品被披露存在多个安全漏洞，攻击者可以利用漏洞构建恶意 WEB 页，诱使用户解析，获得敏感信息或执行任意代码。

CNVD 收录的相关漏洞包括：IBM Rational AppScan FILE URI 信息泄露漏洞、IBM Rational AppScan 导入作业信息泄露漏洞、IBM Rational AppScan 企业平台验证代码执行漏洞、IBM Rational ClearQuest 'cqole.dll' ActiveX 控件堆缓冲区溢出漏洞、IBM Rational AppScan 企业平台服务账户会话劫持漏洞、IBM Rational AppScan 控制台客户端欺骗漏洞、IBM Rational AppScan 文件上传漏洞、IBM Rational AppScan 配置信息泄露漏洞等。

其中，“IBM Rational AppScan FILE URI 信息泄露漏洞”、“IBM Rational AppScan 导入作业信息泄露漏洞”、“IBM Rational AppScan 企业平台验证代码执行漏洞”、“IBM Rational ClearQuest 'cqole.dll' ActiveX 控件堆缓冲区溢出漏洞”的综合评级均为“高危”。目前，IBM 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=48084

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48085

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48089

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47857

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48076

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48077

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48081

http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48098

3、Asterisk 安全漏洞

Asterisk 是一款开放源代码的软件 VoIP PBX 系统。本周，该产品被披露存在多个安全漏洞，攻击者可以利用漏洞发起远程缓冲区溢出攻击，可能导致执行任意代码或拒绝服务。CNVD 收录的相关漏洞包括：Asterisk Skinny Channel Drive 堆缓冲区溢出漏洞、Asterisk Shell 命令执行安全绕过漏洞、Asterisk SIP Channel Driver 拒绝服务漏洞。其中，

“Asterisk Skinny Channel Drive 堆缓冲区溢出漏洞”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=47901
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47897
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=47899

4、Drupal 产品安全漏洞

Drupal 是一款网站内容管理系统。本周，Drupal 的多个模块被披露存在多个漏洞，攻击者可以利用漏洞绕过安全限制执行未经授权的操作，获得敏感信息或执行任意 PHP 代码。CNVD 收录的相关漏洞包括：Drupal 真实姓名模块跨站脚本漏洞、Drupal Linkit 模块访问安全绕过漏洞、Drupal Ubercar 模块跨站脚本漏洞、Drupal Ubercar 模块本地信息泄露漏洞、Drupal Ubercar 模块远程 PHP 代码执行漏洞、Drupal Site Documentation 模块信息泄露漏洞。目前，除“Drupal 真实姓名模块跨站脚本漏洞”外，厂商已经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=48117
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48126
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48132
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48133
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48134
http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=48255

5、PHP Volunteer Management SQL 注入漏洞

PHP Volunteer Management 是一个开源的 Web 应用程序或脚本。本周，PHP Volunteer Management 被披露存在一个综合评级为“高危”的 SQL 注入漏洞，主要影响 1.0.2 版本。攻击者可以利用漏洞访问或修改敏感数据。目前，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=48124

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-2012-1516	Joomla!组件 ccNewsletter 'id' 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漏洞通过注入任意 SQL 代码操纵 SQL 查询： http://www.chillcreations.com/joomla-extensions/ccnewsletter-joomla-newsletter-extension.html

CNVD-2012-1 1519	Discuz!远程代码执行漏洞	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。避免可导致远程任意代码执行： http://discuz.com
CNVD-2012-1 1537	concrete5 SQL 注入漏洞	高	暂无
CNVD-2012-1 1524	PHP Volunteer Management SQL 注入漏洞	高	暂无
CNVD-2012-1 1469	多个 JustSystems 产品缓冲区溢出漏洞	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.justsystems.com/products/index.html
CNVD-2012-1 1459	Xunlei Thunder 不安全库装载任意代码执行漏洞	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。避免攻击者可以构建恶意文件，放置在远程 WebDAV 或 SMB 共享上诱使用户解析，可以目标用户上下文执行任意代码： http://dl.xunlei.com/index.htm?tag=1
CNVD-2012-1 1505	Ettercap 'exchndl.dll'和'quserex.dll' DLL 装载任意代码执行漏洞	高	暂无
CNVD-2012-1 1431	EMC Data Protection Advisor 拒绝服务漏洞（CNVD-2012-11431）	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。避免攻击者可利用漏洞使应用崩溃： http://www.emc.com/products/storage_management/navisphere.jsp
CNVD-2012-1 1482	MediaXxx Mobile Video Module 'query'参数 SQL 注入漏洞	高	暂无
CNVD-2012-1 1432	F5 FirePass sudo 文件 root 空口令漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Mozilla 发布了 14 项安全更新，修复了 Firefox、Thunderbird、SeaMonkey 中存在的 33 个安全漏洞。利用上述漏洞，攻击者可以应用程序上下文执行任意代码、发起钓鱼攻击、窃取敏感信息或导致应用程序崩溃。IBM、Asterisk、Drupal 等的多款应用于安全测试、网站服务器管理的应用软件被披露存在多个漏洞，攻击者可以利用漏洞绕过安全限制执行未经授权的操作、获得敏感信息或任意代码，需引起安全管理员、

系统管理员的关注。

此外，国内外应用广泛的 BBS 建站软件 Discuz! 被披露存在高危漏洞，厂商已经及时给出了修复措施和解决方案，请使用相关产品的用户注意加强防范。

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、Microsoft 发布升级程序，修补 .NET Framework 安全漏洞

本周，Microsoft 发布升级程序，修补了 .NET Framework 存在的安全漏洞。Microsoft .NET Framework 被披露存在参数校验远程整数溢出漏洞，攻击者可以利用漏洞触发堆缓冲区溢出、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=16472

本周要闻速递

1. 微软修复 Hotmail 安全漏洞

微软紧急发布一个补丁，修复 Hotmail 网络邮件服务中的一个严重的安全漏洞。这个安全漏洞能够让黑客重置 Hotmail 账户的口令，使其拥有者无法登录并且让攻击者访问那个用户的收件箱。微软发布这个补丁是因为一些黑客已经在网络上积极地利用这个安全漏洞。一个安全新闻网站报道称，一些黑客正以每个账户 20 美元的价格提供攻破 Hotmail 账户的服务。目前还不清楚有多少 Hotmail 账户遭到黑客利用这个安全漏洞的攻击。不过，遭到攻击的用户会知道，因为这些用户发现他们无法访问自己的 Hotmail 账户。由于这个安全漏洞被积极地利用，微软用一天多的时间找到了修复这个安全漏洞的方法并且更新了 Hotmail。现在，黑客在操纵数据交换的时候会得到一个报错的信息。微软对于这个安全补丁发表了一个简短的声明称，用户不需要采取进一步的措施。

参考链接：<http://article.pchome.net/content-1496581.html>

2. 无线网络出现漏洞

近日，深圳两家国内市场主流的无线设备厂家被曝所生产的某些型号及批次的无线路由器存在 WPS (Wi-Fi Protected Setup, 无线保护设置) 无线安全漏洞，用户如果使用了这些产品的默认安全设置，则其无线网络的加密密码可以被轻松猜解，信息泄露的大门也随之洞开。WPS 是 Wi-Fi 联盟于 2007 年发布的一个认证，目的是让用户可以通过“一键化设定”的简单方式来设定无线网络装置，并保证具备一定的安全性。WPS 通常使用 PIN 码作为无线网络的默认密码，用户开启 WPS 功能后，在接入的无线终端上

输入 PIN 码（默认无线网络密码），就可以实现快捷方便的无线上网功能，然而，便捷的背后却隐藏着信息泄露的巨大风险。本次暴露出安全漏洞的两个厂商也采用了上述方式，但是其 PIN 码（默认无线网络密码）却并非通过随机算法生成，而是直接通过无线路由器的硬件 ID（出厂 MAC 地址）换算得来。其中某厂商设备的无线路由器，甚至基本不需猜解，只需将 MAC 地址的 3 个低字节进行 16 进制到 10 进制的转换，即可获得 8 个 PIN 码数字中的 7 个，意味着攻击者如果想通过该无线路由器接入网络，只需做 10 次尝试即可。该漏洞与之前披露出的国外某无线路由器厂商的 WPS 漏洞原理基本相同，都是 PIN 码生成算法不严谨，且与 MAC 地址存在关联性，使得攻击者很容易猜解出 PIN 码。

参考链接：<http://money.163.com/12/0427/11/803GSQFK00253B0H.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