国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2013 年 04 月 01 日-2013 年 04 月 07 日 **2013 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低。

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 101 个，其中高危漏洞 33 个、中危漏洞 63 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 96 个。本周收录的漏洞中，已有 62 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“Pollen CMS 'index.php'本地文件包含漏洞”、“KNet Web Server 缓冲区溢出漏洞”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及个人报送了本周收录的全部 101 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、天融信等单位报送数量较多。此外，奇虎公司、High-Tech Bridge Security Research Lab 以及个人报送者向 CNVD 提交了 9 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	54	0
绿盟科技	31	0
安天实验室	25	0
天融信	53	0
恒安嘉新	30	0
东软	4	0
High-Tech Bridge Security Research Lab	3	3
奇虎 360	3	3

个人	1	3
报送总计	204	9
录入总计	101（去重）	9

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、Wordpress、PostgreSQL、IBM 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	13	13%
2	Wordpress	6	6%
3	PostgreSQL	5	5%
4	IBM	5	5%
5	Cisco	4	4%
6	HP	2	2%
7	Advanced Media Technologie	2	2%
8	MantisBT	2	2%
9	Novell	1	1%
10	Red Hat	1	1%
11	其它	60	59%

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 101 个漏洞。其中应用程序漏洞 58 个，WEB 应用漏洞 31 个，网络设备漏洞 5 个，数据库漏洞 5 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	58
WEB 应用漏洞	31
网络设备漏洞	5
数据库漏洞	5
安全产品漏洞	2
操作系统漏洞	0

表 3 漏洞按影响类型统计表

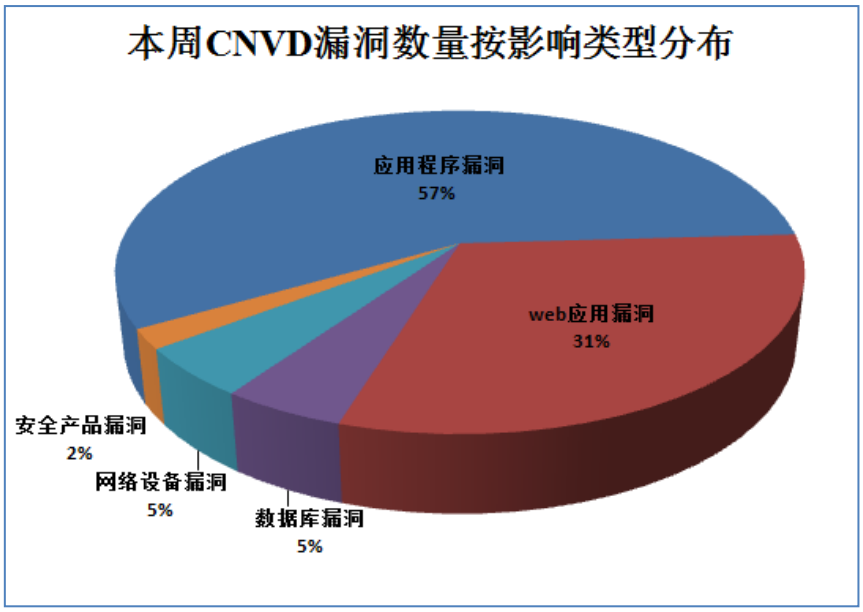

图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 5 个网络设备漏洞：Advanced Media Technologie 多个产品内部 IP 地址信息泄露漏洞、Advanced Media Technologie 多个产品远程未授权重启漏洞、NetGear WNR1000 路由器验证绕过漏洞、思科 Linksys EA2700 路由器产品密码更改漏洞、思科 Linksys EA2700 路由器产品权限绕过漏洞。其中，“Advanced Media Technologie 多个产品远程未授权重启漏洞”的综合评级为“高危”，相关厂商已经发布了漏洞修补程序。

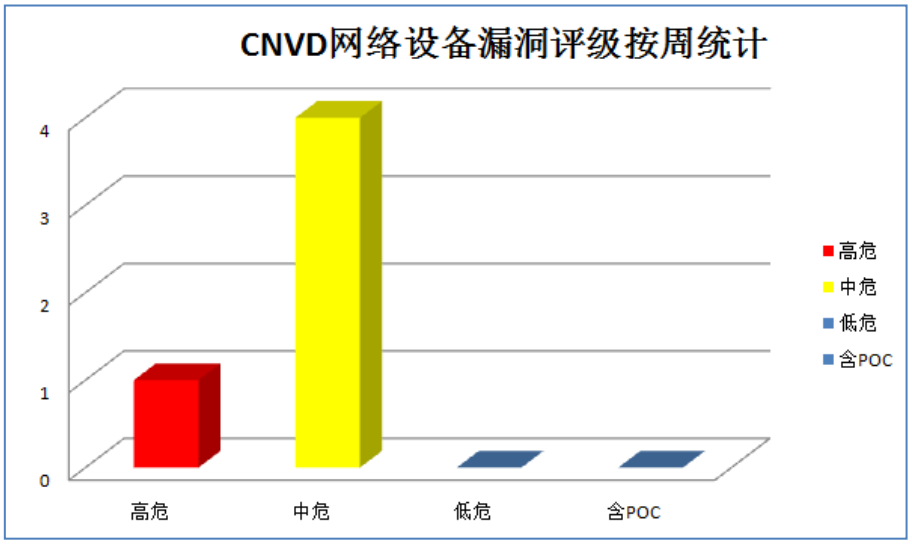

图 2 网络设备漏洞统计

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、Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可提升权限，导致应用程序崩溃或远程执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla 多个产品 Mesa 图形驱动 WebGL 崩溃漏洞、Mozilla 多个产品 SOW 保护绕过节点克隆漏洞、Mozilla 多个产品存在未明内存漏洞（CNVD-2013-21636、CNVD-2013-21637）、Mozilla 多个产品插件存在未明栈破坏漏洞、Mozilla 多个产品 NSS 库越界读漏洞、Mozilla 多个产品 Mozilla Updater 权限提升漏洞、Mozilla 多个产品灰度模式 PNG 图像渲染内存泄露漏洞等。上述漏洞中“Mozilla 多个产品 Mesa 图形驱动 WebGL 崩溃漏洞、Mozilla 多个产品 SOW 保护绕过节点克隆漏洞、Mozilla 多个产品存在未明内存漏洞（CNVD-2013-21636、CNVD-2013-21637）、Mozilla 多个产品插件存在未明栈破坏漏洞”的综合评级均为“高危”。厂商已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/flaw/show/CNVD-2013-21644

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21643

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21636

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21637

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21638

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21648

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21645

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21640

2、PostgreSQL 安全漏洞

PostgreSQL 是一款对象关系型数据库管理系统，支持扩展的 SQL 标准子集。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可绕过安全限制，修改配置，发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：PostgreSQL 'contrib/pgcrypto'函数信息泄露漏洞、PostgreSQL 不安全临时文件创建漏洞、PostgreSQL 密码泄露漏洞、PostgreSQL 安全绕过漏洞、PostgreSQL 拒绝服务漏洞。上述漏洞中“PostgreSQL 'contrib/pgcrypto'函数信息泄露漏洞、PostgreSQL 不安全临时文件创建漏洞、PostgreSQL 密码泄露漏洞”的综合评级均为“高危”。厂商已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/flaw/show/CNVD-2013-21786

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21788

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21784

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21787

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21781

3、IBM 产品安全漏洞

IBM Lotus iNotes 是一款 Web 应用解决方案；IBM InfoSphere Replication Server 用于对系统提供数据复制、集成和同步等功能；IBM InfoSphere Information Server 是一款数据集成软件平台；IBM Netezza 是一款数据仓库应用设备。本周，上述 IBM 产品被披露存在多个安全漏洞，攻击者利用漏洞获得敏感信息，劫持用户会话，或执行任意代码。

CNVD 收录的相关漏洞包括：IBM Netezza Performance Portal 目录信息泄露漏洞、IBM InfoSphere Information Server 跨站脚本漏洞、IBM InfoSphere Replication Server 信息泄露漏洞、IBM Lotus iNotes 共享邮件文件存在多个本地跨站脚本漏洞、IBM Lotus iNotes 存在未明跨站脚本漏洞。厂商已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/flaw/show/CNVD-2013-21633

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21591

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21592

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21454

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21455

4、Cisco 产品安全漏洞

Cisco Connected Grid Network Management System 是一款智能电网通信网络执行生命周期管理软件。本周，上述思科产品被披露存在多个安全漏洞，攻击者利用漏洞获得敏感信息，劫持用户会话，执行数据库操作。

CNVD 收录的相关漏洞包括： Cisco Connected Grid Network Management System (CG-NMS) SQL 注入漏洞、Cisco Connected Grid Network Management System (CG-NMS) 跨站脚本漏洞。厂商已发布了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/flaw/show/CNVD-2013-21585

http://www.cnvd.org.cn/flaw/show/CNVD-2013-21586

5、KNet Web Server 缓冲区溢出漏洞

KNet Web Server 是一款 WEB 服务程序。本周，该产品被披露存在一个综合评级为“高危”的缓冲区溢出漏洞。由于 KNet Web Server 未能正确过滤用户提交的请求，攻击者利用漏洞可提交恶意请求进行缓冲区溢出攻击，执行任意代码。目前，互联网上已经出现了针对该漏洞的攻击代码，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/flaw/show/CNVD-2013-21588

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/flaw/list.htm

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2013-21761	askiaweb 存在多个 SQL 注入漏洞	高	暂无
CNVD-2013-21769	FUDforum PHP 代码执行漏洞	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://fudforum.svn.sourceforge.net/fudforum/?rev=5596&view=rev
CNVD-2013-21767	ownCloud 'addressbookprovider.php' SQL 注入漏洞	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://owncloud.org/about/security/advisories/oC-SA-2013-012/
CNVD-2013-21782	CensorNet 'Create/Manage Reports' SQL 注入漏洞	高	暂无
CNVD-2013-21616	HP System Management Homepage 'iprange'参数远程代码执行漏洞	高	暂无
CNVD-2013-21655	Virtual Access Monitor SQL 注入漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息：http://www.virtualaccess.com/customer-support.php
CNVD-2013-21617	KindEditor 存在多个文件上传漏洞	高	暂无
CNVD-2013-21583	AKFAvatar 存在多个未明漏洞	高	AKFAvatar 0.23.1 已经修复此漏洞，建议用户下载更新：http://akfavatar.nongnu.org/
CNVD-2013-21582	Advanced Media Technologie 多个产品远程未授权重启漏洞	高	暂无
CNVD-2013-21601	ClipShare 存在多个 SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Mozilla 多款产品被披露存在多个安全漏洞，攻击者利用漏洞有可能发起大规模网页挂马攻击。PostgreSQL 数据库管理系统以及 Cisco 和 IBM 多款产品也被披露存在多个漏洞，相关企业用户应重点加强防范。此外，KNet Web Server 被披露

存在零日漏洞，相关用户应随时关注厂商主页，及时获取修复补丁或解决方案。

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、HP 发布升级程序，修补 System Management Homepage 安全漏洞

HP System Management Homepage 是一款 HP 公司发布的系统管理套件。本周，HP 发布升级程序，修补了 System Management Homepage 存在的漏洞。远程攻击者可利用漏洞以 WEB 权限执行任意代码。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/patchInfo/show/33104

本周要闻速递

1. 英特尔全力修复部分 Haswell USB3.0 漏洞

英特尔 Intel 本月 5 日发表声明证实，与 Haswell 处理器配套的芯片组存在一个 USB 漏洞，目前正将尽快修复这个 Bug。据悉，该漏洞会造成 USB 3.0 在进入待机状态后消失，某些情况下，用户必须将设备拔出之后再次插上，系统才能重新识别到 USB3.0 设备。但是英特尔同时也证实，这一“非重要错误”并不会造成数据损坏或丢失。据英特尔发布的产品变更通知称，公司将在 2013 年 4 月 19 日向客户提供修复该漏洞的芯片组样品，最终，英特尔计划从 7 月 15 日起向客户提供修复了漏洞的最终版芯片组。

参考链接：http://notebook.it168.com/a2013/0407/1469/000001469375.shtml

2. Auxo 1.4 版本更新修复漏洞

Auxo 作为越狱社区最具人气的 iOS 应用切换器的替代品，日前已经获得了一次重大更新，带来新的切换开关，修复漏洞等。Auxo 1.4 修复音频播放崩溃问题，LiveClock 兼容性问题，封堵蓝牙配对漏洞，修复各种崩溃问题，提高速度和内存性能。

参考链接：http://tech.ifeng.com/digi/mobile/soft/ios/detail_2013_04/07/23934858_0.shtml

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