

信息安全漏洞周报

2014 年 6 月 30 日-2014 年 7 月 6 日

2014 年第 27 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 149 个，其中高危漏洞 31 个、中危漏洞 102 个、低危漏洞 16 个。上述漏洞中，可利用来实施远程攻击的漏洞有 128 个。本周收录的漏洞中，已有 116 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“Baidu Spark 浏览器栈溢出拒绝服务漏洞”等零日攻击代码，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、合作伙伴及个人报送了本周收录的全部 149 个漏洞。报送情况如表 1 所示。其中，启明星辰、奇虎 360、绿盟科技、天融信、安天实验室等单位报送数量较多。此外，CNCERT 各分中心、习科网络安全、汉柏科技有限公司、High-Tech Bridge Security Research 及白帽子向 CNVD 提交了 208 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	124	0
奇虎 360	119	119
绿盟科技	100	0
天融信	97	0
安天实验室	93	0
恒安嘉新	65	0

知道创宇	2	1
习科网络安全	51	50
汉柏科技有限公司	2	2
CNCERT 江西分中心	8	8
CNCERT 山西分中心	6	6
CNCERT 山东分中心	4	4
CNCERT 安徽分中心	3	3
CNCERT 湖南分中心	3	3
CNCERT 湖北分中心	2	2
CNCERT 宁夏分中心	1	1
CNCERT 贵州分中心	1	1
High-Tech Bridge Security Research	2	2
个人	6	6
报送总计	689	208
录入总计	149（去重）	208

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Apple、WordPress、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	Apple	29	19%
2	WordPress	22	15%
3	IBM	13	9%
4	WebKit	10	7%
5	PHP	6	4%
6	Linux	5	3%
7	EMC	4	3%
8	Cisco	3	2%
9	Symantec	2	1%
10	其他	55	37%

表 2 漏洞产品涉及厂商分布统计表

本周，CNVD 收录了 149 个漏洞。其中应用程序漏洞 79 个，WEB 应用漏洞 36 个，操作系统漏洞 28 个，网络设备漏洞 4 个，安全产品漏洞 1 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	79
WEB 应用漏洞	36
操作系统漏洞	28
网络设备漏洞	4
安全产品漏洞	1
数据库漏洞	1

表 3 漏洞按影响类型统计表

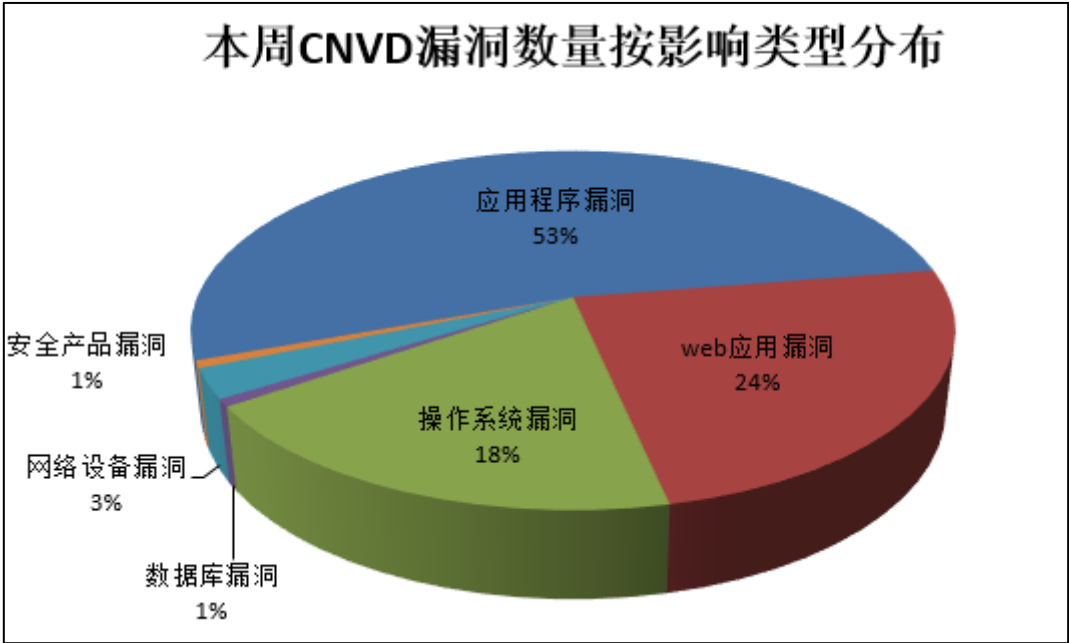


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 7 个电信行业漏洞，9 个移动互联网漏洞（如下图表所示）。其中，“discuz! 7.x faq.php SQL 注入漏洞”的综合评级均为“高危”。相关厂商已经发布了上述漏洞的修补程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2014-03933	IBM WebSphere Application Server 远程信息泄露漏洞	中	是
电信	CNVD-2014-03956	IBM WebSphere Application Server 存在未明信息泄露漏洞（CNVD-2014-03956）	中	是
电信	CNVD-2014-03957	IBM WebSphere Application Server 存	中	是

		在未明信息泄露漏洞（CNVD-2014-03957）		
电信	CNVD-2014-03985	Thomson TWG87OUIR Router '/goform/RgSecurity'跨站请求伪造漏洞	低	是
电信	CNVD-2014-04028	discuz! 7.x faq.php SQL 注入漏洞	高	是
电信	CNVD-2014-04030	IBM Tivoli Application Dependency Discovery Manager 目录遍历漏洞	低	是
电信	CNVD-2014-04041	Comtrend CT-5361T ADSL 路由器'password.cgi'密码泄露漏洞	高	否
移动互联网	CNVD-2014-04027	Apple iOS Webkit 地址栏伪造漏洞	中	是
移动互联网	CNVD-2014-04026	Apple iOS 邮件附件泄露漏洞	低	是
移动互联网	CNVD-2014-04025	Apple iOS safari 非法 URL 处理漏洞	中	是
移动互联网	CNVD-2014-04024	Apple iOS 未授权禁用 Find My iPhone 漏洞	中	是
移动互联网	CNVD-2014-04023	Apple iOS Siri 处理联系人信息泄露漏洞	低	是
移动互联网	CNVD-2014-04022	Apple iOS 密码尝试限制绕过漏洞	低	是
移动互联网	CNVD-2014-04021	Apple iOS 飞行模式状态管理错误漏洞	低	是
移动互联网	CNVD-2014-04020	Apple iOS CoreGraphics XBM 文件处理任意代码执行漏洞	中	是
移动互联网	CNVD-2014-04019	Apple iOS 设备激活安全绕过漏洞	低	是

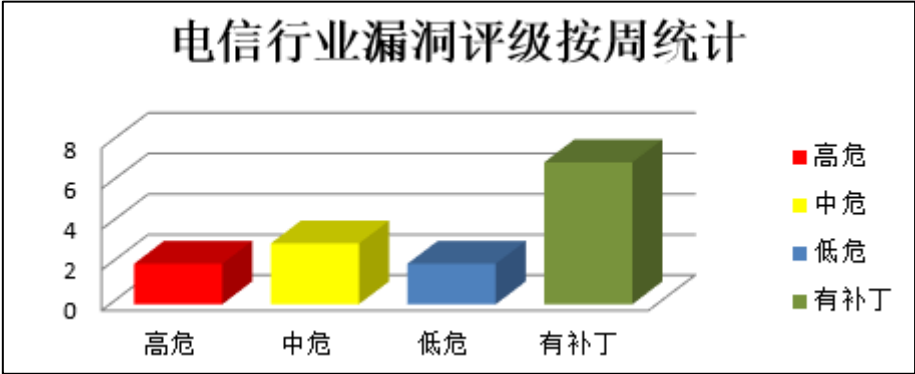


图 1 电信行业漏洞统计

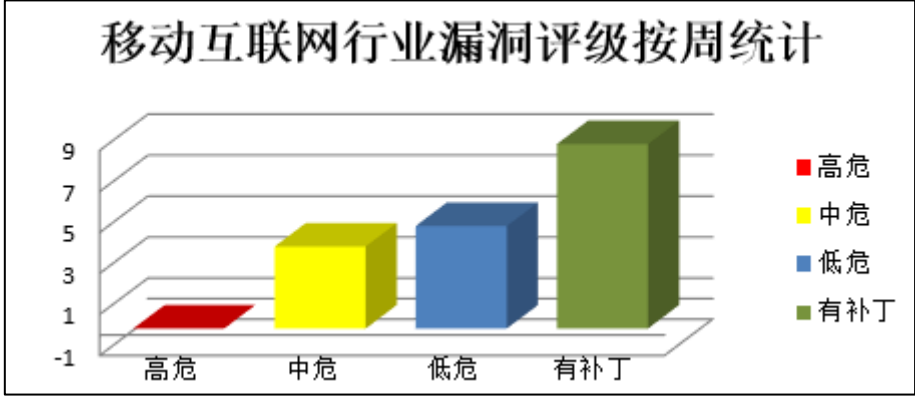


图 2 移动互联网行业漏洞统计



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、Discuz! 产品安全漏洞

Discuz! 是一款国内流行的社区论坛平台。本周，上述产品被披露存在 SQL 注入漏洞，攻击者可利用漏洞获取数据库敏感信息。

CNVD 收录的相关漏洞包括：discuz! 7.x faq.php SQL 注入漏洞。上述漏洞的综合评级均为“高危”。目前，互联网上已经出现了针对该漏洞的攻击代码，厂商已经发布了上述漏洞的修补程序。CNVD 提醒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-2014-04028>

2、Apple 产品安全漏洞

Apple Mac OS X 是一款苹果公司开发的操作系统。本周，上述产品被披露存在拒绝服务和任意代码执行漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apple OS X 拒绝服务漏洞（CNVD-2014-04048、CNVD-2014-04055）、Apple OS X 任意代码执行漏洞（CNVD-2014-04050、CNVD-2014-04052、CNVD-2014-04053）。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒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-2014-04048>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04055>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04050>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04052>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04053>

3、IBM 产品安全漏洞

IBM AIX 是一款商业性质的操作系统。IBM Marketing Platform 是美国 IBM 公司的一套营销平台。IBM WebSphere Application Server (WAS) 是美国 IBM 公司开发并发行的一款应用服务器产品，它是 Java EE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、执行未经授权操作或提升权限。

CNVD 收录的相关漏洞包括：IBM AIX 权限提升漏洞、IBM Marketing Platform 会话劫持漏洞、IBM Marketing Platform 存在未明 SQL 注入漏洞、IBM WebSphere Application Server 存在未明信息泄露漏洞（CNVD-2014-03957、CNVD-2014-03956）。其

中“IBM AIX 权限提升漏洞”的综合评级为“高危”。目前，厂商已经发布了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/flaw/show/CNVD-2014-04073>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04045>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03958>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03957>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03956>

4、WordPress 产品安全漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞注入任意 Web 脚本或 HTM 代码。

CNVD 收录的相关漏洞包括：WordPress 插件 World of Warcraft - Armory Table 存在未明漏洞、WordPress 插件 DMCA WaterMarker 跨站脚本漏洞、WordPress 插件 dsIDXpress IDX 跨站脚本漏洞、WordPress Theme My Login 插件本地文件包含漏洞、WordPress Simple Share Buttons Adder 插件存在多个安全绕过漏洞。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户及时下载补丁更新，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-2014-04044>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04061>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04062>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03976>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03936>

5、Comtrend CT-5361T ADSL 路由器'password.cgi'密码泄露漏洞

Comtrend CT-5361T ADSL Router 是康全电讯（Comtrend）公司的一款 ADSL 路由器产品。本周，Comtrend CT-5361T ADSL Router 被披露存在综合评级为“高危”的密码泄露漏洞。攻击者可以利用漏洞获取敏感信息。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/flaw/show/CNVD-2014-04041>

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-2014-03935	SQLite 存在未明缓冲区溢出漏洞	高	用户可以联系供应商获得补丁信息： http://www.sqlite.org/

CNVD-2014-03934	Memcached 存在多个堆缓冲区溢出漏洞	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://memcachedb.org/
CNVD-2014-03948	Piwigo 'picture_modify.php' SQL 注入漏洞	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://piwigo.org/
CNVD-2014-03947	Openfiler 存在多个漏洞	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.openfiler.com/
CNVD-2014-03952	Foxit PDF SDK DLL 'FPDFBookmark_GetTitle()'缓冲区溢出漏洞	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.foxitsoftware.com/support/security_bulletins.php#FRD-20
CNVD-2014-03964	LZ4 'lz4.c'内存破坏漏洞	高	用户可以联系供应商获得补丁信息： http://www.securityfocus.com/bid/68218/solution
CNVD-2014-03972	Exim 'dmarc.c'远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： http://www.exim.org/
CNVD-2014-03984	Mailspect Control Panel 存在多个漏洞	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.mailspect.com/
CNVD-2014-03988	FFmpeg LZO 'LZ4_decompress_generic()'函数内存破坏漏洞	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://libav.org/
CNVD-2014-03989	Libav LZO 'av_lzo1x_decode'函数内存破坏漏洞	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.libav.org/

表 3 部分高危漏洞列表

小结：本周，Discuz!产品被披露存在多个漏洞，攻击者可利用漏洞获取数据库敏感信息。此外，Apple、IBM、WordPress 多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码，获取敏感信息或执行未经授权操作。另外，Comtrend 被披露存在一个高危零日漏洞。攻击者可以利用漏洞获取敏感信息。建议相关用户应随时关注上述厂商主页，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、FFmpeg 修补 LZO 'LZ4_decompress_generic()'函数漏洞

FFmpeg 是一款用于录制、转换和流化音频和视频的完整解决方案。

本周，FFmpeg 修补了本产品存在的内存破坏漏洞，避免攻击者利用漏洞进行整数溢出攻击，可使应用程序崩溃或执行任意代码。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网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/46927>

本周要闻速递

1. 安卓设备再曝安全漏洞

7 月 4 日消息，据国外媒体报道，电子前线基金会发现安装了安卓 3.1 或以上系统的设备处于 PNO(Preferred Network Offload)模式时，该设备就会发送它最近连接过的 Wi-Fi 网络信息。任何连上同一 Wi-Fi 网络的人则都可以看到这些信息，还可能根据你最近连接过的 Wi-Fi 网络了解到你的行踪。

参考链接：<http://tech.sina.com.cn/t/2014-07-04/11189476647.shtml>

2. 赛门铁克软件涉“高危安全漏洞”

日前，网络上传出一份落款为公安部科技信息化局的通知。该份通知显示，因赛门铁克的“数据防泄漏”(Symantec DLP)产品存在窃密后门和高危安全漏洞，各地公安机关正在核查赛门铁克“数据防泄漏”、防病毒等安全产品的使用情况。同时，通知要求各级公安机关今后禁止采购使用该产品。对于已在使用相关产品的单位，在接到通知后，要立即停用此产品，并列出时间表，尽快用国产软件予以更换。

参考链接：<http://zici.org/articles/2014-7/2014-7-3/23320329.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

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999