

信息安全漏洞周报

2014 年 5 月 12 日-2014 年 5 月 18 日

2014 年第 20 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 123 个，其中高危漏洞 49 个、中危漏洞 63 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 107 个。本周收录的漏洞中，已有 98 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“Joomla! Inneradmission 组件'index.php' SQL 注入漏洞”、“BlazeVideo BlazeDVD Pro '.PLF' 文件远程栈缓冲区溢出漏洞”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 5 家成员单位、合作伙伴及个人报送了本周收录的全部 123 个漏洞。报送情况如表 1 所示。其中，绿盟科技、天融信、启明星辰、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、High-Tech Bridge Security Research Lab 及多个白帽子向 CNVD 提交了 98 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
绿盟科技	156	0
天融信	134	0
启明星辰	124	0
安天实验室	123	0
恒安嘉新	37	0
习科网络安全	60	60
CNCERT 山西分中心	10	10

CNCERT 贵州分中心	9	9
CNCERT 江西分中心	5	5
CNCERT 贵州分中心	2	2
CNCERT 福建分中心	2	2
CNCERT 山东分中心	1	1
CNCERT 安徽分中心	1	1
High-Tech Bridge Security Research Lab	3	3
个人	5	5
报送总计	672	98
录入总计	123（去重）	98

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、MediaWiki 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	Adobe	15	14%
2	Microsoft	13	11%
3	MediaWiki	10	8%
4	WordPress	7	6%
5	Google	4	3%
6	Linux	4	3%
7	Red Hat	3	2%
8	D-Link	2	2%
9	Cisco	1	1%
10	其他	64	50%

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 123 个漏洞。其中应用程序漏洞 86 个，WEB 应用漏洞 20 个，操作系统漏洞 8 个，网络设备漏洞 8 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	86
WEB 应用漏洞	20

操作系统漏洞	8
网络设备漏洞	8
安全产品漏洞	1

表 3 漏洞按影响类型统计表

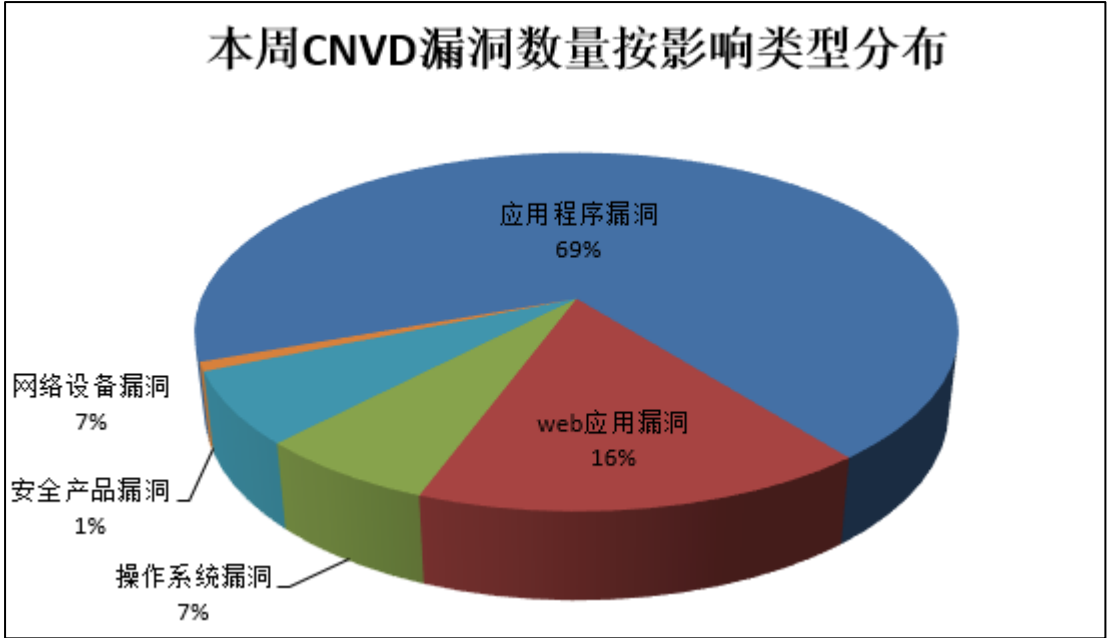


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周,CNVD 收录了 7 个电信行业漏洞、1 个移动互联网行业漏洞(如下列表所示)。其中,“ISC BIND prefetch 功能拒绝服务漏洞”的综合评级为“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-2014-02933	ISC BIND prefetch 功能拒绝服务漏洞	高	是
电信	CNVD-2014-02944	Huawei Quidway S-Series Sw itches 拒绝服务漏洞	中	是
电信	CNVD-2014-02961	D-Link DAP-1320 'html_respo nse_message'跨站脚本漏洞	中	是
电信	CNVD-2014-02960	D-Link DAP-1350 SQL 注入漏洞	中	是
电信	CNVD-2014-02957	HP H-series Fibre Channel S witches 远程信息泄露漏洞	低	是
电信	CNVD-2014-03004	Cisco IOS 软件远程拒绝服务漏洞	中	是

电信	CNVD-2014-03045	Huawei Campus Series Switches 存在多个漏洞	中	是
移动互联网	CNVD-2014-02995	Google Android OS 存在漏洞	中	是

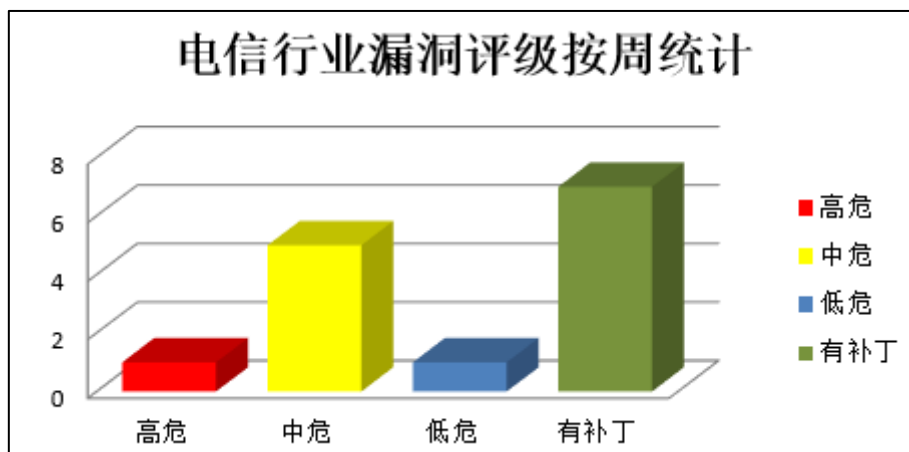


图 1 电信行业漏洞统计

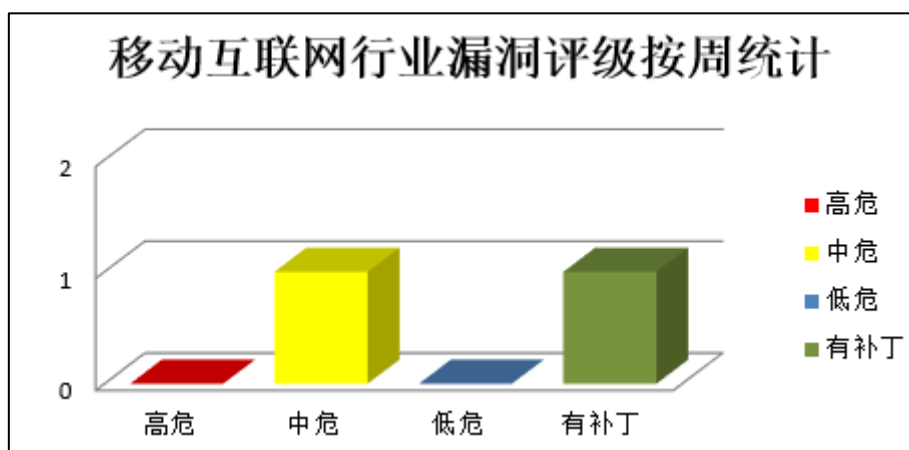


图 2 移动互联网行业漏洞统计

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、Microsoft 产品安全漏洞

Microsoft SharePoint Server 是一款服务器功能集成套件，提供全面的内容管理和企业搜索、加速共享业务流程并便利跨界限信息共享。Microsoft Internet Explorer 是一款 WEB 浏览器。Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞构建恶意 WEB 页，诱使用户解析，可以应用程序上下文执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Office Web Apps 远程代码执行漏洞、Microsoft Internet Explorer 存在未明内存破坏漏洞（CNVD-2014-03043、CNVD-2014-0304

4)、Microsoft Windows 'Windows Shell'处理程序本地权限提升漏洞、Microsoft SharePoint 存在多个远程代码执行漏洞。上述漏洞的综合评级均为“高危”。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-2014-03041>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03043>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03044>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02992>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02982>

2、Adobe 产品安全漏洞

Adobe Reader/Acrobat 是流行的处理 PDF 文件的应用程序。Adobe Flash Player 是一款 Flash 文件处理程序。Adobe Air 是一款 Adobe 公司出品的跨操作系统的运行时库。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞构建恶意文件，诱使用户解析，以应用程序上下文执行任意代码或绕过安全限制。

CNVD 收录的相关漏洞包括：Adobe Reader / Acrobat 存在未明缓冲区溢出漏洞（CNVD-2014-03049）、Adobe Reader / Acrobat 存在未明内存错误引用漏洞、Adobe Reader / Acrobat API 调用处理代码执行漏洞、Adobe Flash Player / AIR 存在未明安全绕过漏洞（CNVD-2014-02987、CNVD-2014-02988）。上述漏洞的综合评级均为“高危”。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-2014-03049>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02984>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02999>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02987>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02988>

3、Google 产品安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞构建恶意 WEB 页，诱使用户解析，可引用释放内存，以应用程序上下文执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome WebSockets 远程代码执行漏洞、Google Chrome 远程代码执行漏洞（CNVD-2014-03047）、Google Chrome DOM ranger 整数溢出漏洞、Google Android OS 存在漏洞。其中，除“Google Android OS 存在漏洞”外，其余漏洞的综合评级均为“高危”。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-2014-03046>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03047>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03048>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02995>

4、X.Org 产品安全漏洞

X.Org 是 X.Org Foundation 对 X 窗口系统的开源实现。本周，上述产品被披露存在缓冲区溢出和整数溢出漏洞，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：X.Org LibXfont 存在缓冲区溢出漏洞、X.Org LibXfont 存在多个整数溢出漏洞（CNVD-2014-03036、CNVD-2014-03038）。上述漏洞的综合评级均为“高危”。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-2014-03037>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03036>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03038>

5、eazyCMS 'index.php' SQL 注入漏洞

eazyCMS 是一套内容管理系统。该系统支持自定义网站、所见即所得网页编辑器和网站维护等。本周，eazyCMS 被披露存在综合评级为“高危”的 SQL 注入漏洞。由于程序在构造 SQL 查询语句之前未能充分过滤用户提交的数据，攻击者可利用漏洞控制应用程序，访问或修改数据。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-2014-02936>

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-2014-02933	MediaWiki Scribunto 扩展缓冲区溢出漏洞	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://lists.wikimedia.org/pipermail/mediawiki-announce/2014-January/000138.html
CNVD-2014-02934	多个 F5 BIG-IP 产品远程命令注入漏洞	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://support.f5.com/kb/en-us/solutions/public/15000/200/sol15220.html
CNVD-2014-02950	AVG Remote Administration 'ClientLibraryName'参数远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载： http://download.avg.com/filedir/inst/avg_rad_x86_all_2013_2895.exe

CNVD-2014-02951	Collabtive 'managefile.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://www.collabtive.o-dyn.de/blog/?p=225
CNVD-2014-02955	VMTurbo Operations Manager 目录遍历漏洞	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.vmturbo.com
CNVD-2014-02964	Foreman 代码注入漏洞	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://theforeman.org/security.html#2013-0210
CNVD-2014-03009	EGroupware 'call_user_func()'函数远程代码执行漏洞	高	EGroupware 1.8.007 已修复此漏洞，建议用户下载使用： http://www.egroupware.org/forum#nable-td3997580 http://www.egroupware.org/changelog
CNVD-2014-03016	MediaWiki 输入验证漏洞（CNVD-2014-03016）	高	请安装厂商已发布的最新版本或补丁： http://lists.wikimedia.org/pipermail/mediawiki-announce/2014-January/000138.html
CNVD-2014-03005	QEMU 图形大小验证整数溢出漏洞	高	用户可联系供应商获得补丁信息： http://fabrice.bellard.free.fr/qemu/
CNVD-2014-03006	QEMU 远程代码执行漏洞	高	用户可联系供应商获得补丁信息： http://fabrice.bellard.free.fr/qemu/

表 3 部分高危漏洞列表

小结：本周，Microsoft 披露多个安全产品漏洞，攻击者可利用漏洞构建恶意 WEB 页，诱使用户解析，可以应用程序上下文执行任意代码。此外，Adobe、Google、X.Org 集中披露多款产品存在多个漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。easyCMS 被披露存在一个高危零日漏洞。需要国内用户注意的是，F5 BIG-IP 多款应用交付设备存在远程代码执行高危漏洞。CNVD 已经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、ISC 修补 BIND 产品漏洞

ISC BIND 是一款 DNS 协议的实现。

本周，ISC 修补了上述产品存在的拒绝服务漏洞，避免远程攻击者通过 DNS 请求触发不明属性的响应，导致拒绝服务。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/45489>

本周要闻速递

1. 谷歌用户遭新型钓鱼攻击

据外媒报道，通过一种最新的钓鱼骗局，黑客正将目标对准谷歌用户的密码，和过去的钓鱼攻击比起来，最新的方式更难被检测及拦截。知名安全软件公司 Bitdefender 专家比恩卡·史坦艾斯库表示，“我们此前没有发现过此类网络钓鱼式攻击。它是加强版的，通常安全解决方案会在用户打开网页前阻止恶意活动，但这次，安全解决方案接收到编码内容，却不能有效阻止。”昨日（5月14日），金山安全专家李铁军在接受《每日经济新闻》记者采访时表示，Chrome 浏览器的确存在安全漏洞，谷歌方面需要打个补丁；从用户角度看，使用身份双重验证，同时安全软件也需要相应升级，才能有效避免遭遇钓鱼。

参考链接：http://finance.ifeng.com/a/20140515/12335014_0.shtml

2. 小米被曝安全漏洞

5月15日是小米公司新品发布会的时间，但记者留意到有相当一部分小米人员被紧急调配去处理资料安全工作。原因是早前有网友爆料称小米官网论坛 800 万的用户数据泄露，这一消息昨日在国内安全问题反馈平台乌云网获得证实。根据乌云网公布的信息显示，小米论坛官方数据库泄露涉及 800 万小米论坛注册用户，泄露的数据可进入小米账户，通过小米云服务可得到手机号及设备信息；通过同步可获得通讯录、短信、照片，并可在线定位，锁定手机及擦除信息等。目前，小米公司已经紧急处理此事，并且发布了《账号安全防范公告》提醒论坛用户修改自己的账号密码。

参考链接：<http://tech.sina.com.cn/i/2014-05-15/11059380221.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