

信息安全漏洞周报

2014 年 7 月 7 日-2014 年 7 月 13 日

2014 年第 28 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 168 个，其中高危漏洞 59 个、中危漏洞 95 个、低危漏洞 14 个。上述漏洞中，可利用来实施远程攻击的漏洞有 150 个。本周收录的漏洞中，已有 126 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“Foe CMS 存在多个输入验证漏洞”、“Kerio Control 'print.php'存在多个 SQL 注入漏洞”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 168 个漏洞。报送情况如表 1 所示。其中，安天实验室、恒安嘉新、奇虎 360、启明星辰、天融信等单位报送数量较多。此外，CNCERT 各分中心、习科网络安全及白帽子向 CNVD 提交了 174 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
安天实验室	131	0
恒安嘉新	99	0
奇虎 360	99	99
启明星辰	94	0
天融信	94	0
习科网络安全	12	12

CNCERT 江西分中心	22	22
CNCERT 福建分中心	11	11
CNCERT 安徽分中心	11	11
CNCERT 山西分中心	8	8
CNCERT 广东分中心	4	4
CNCERT 河南分中心	4	4
CNCERT 青海分中心	1	1
个人	2	2
报送总计	592	174
录入总计	168（去重）	174

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 WordPress、Microsoft、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	WordPress	32	19%
2	Microsoft	27	16%
3	IBM	13	8%
4	Cisco	8	5%
5	Electric	7	4%
6	FireEye	6	4%
7	Red Hat	6	4%
8	Linux	4	2%
9	Google	4	2%
10	其他	61	36%

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 168 个漏洞。其中应用程序漏洞 85 个，WEB 应用漏洞 44 个，操作系统漏洞 17 个，网络设备漏洞 10 个，安全产品漏洞 9 个，数据库漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	85
WEB 应用漏洞	44
操作系统漏洞	17

网络设备漏洞	10
安全产品漏洞	9
数据库漏洞	3

表 3 漏洞按影响类型统计表

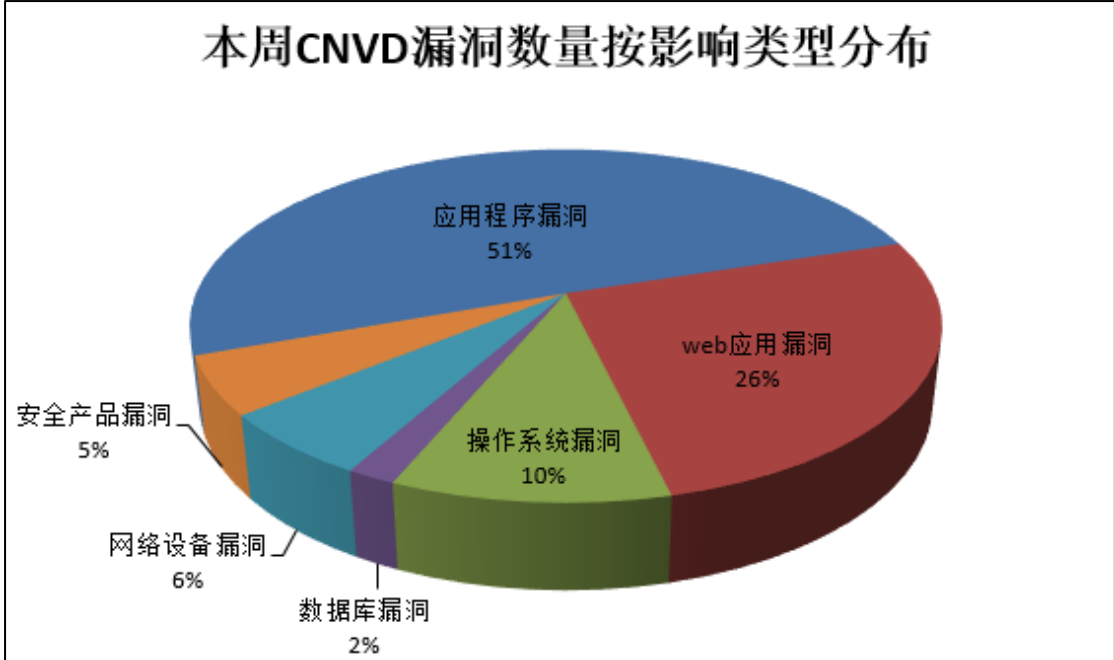


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 15 个电信行业漏洞，3 个移动互联网漏洞，1 个工控行业漏洞（如下图表所示）。其中，“Netgear GS108PE Prosafe Plus Switch 硬编码凭证身份验证绕过漏洞、SYAC TB DigiEye 3G 产品后门未经授权访问漏洞、Yokogawa 多个产品'BKF Sim_vhfd.exe'缓冲区溢出漏洞”的综合评级均为“高危”。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2014-04081	Netgear GS108PE Prosafe Plus Switch 硬编码凭证身份验证绕过漏洞	高	否
电信	CNVD-2014-04080	Cisco ASR 1000 系统路由器拒绝服务漏洞	中	是
电信	CNVD-2014-04091	Electric Sheep Fencing pfSense 跨站脚本漏洞	中	是
电信	CNVD-2014-04090	Electric Sheep Fencing pfSense 跨站脚本漏洞（CNVD-2014-04090）	中	是
电信	CNVD-2014-04089	Electric Sheep Fencing pfSense 会话固定漏洞	中	是
电信	CNVD-2014-04088	Electric Sheep Fencing pfSense 目录遍历漏洞	中	是

电信	CNVD-2014-04087	Electric Sheep Fencing pfSense 绝对路径遍历漏洞	中	是
电信	CNVD-2014-04086	Electric Sheep Fencing pfSense 远程代码执行漏洞	中	是
电信	CNVD-2014-04085	Electric Sheep Fencing pfSense 跨站脚本漏洞（CNVD-2014-04085）	中	是
电信	CNVD-2014-04083	Cisco IOS XR Software Static Punt Policer 拒绝服务漏洞	中	是
电信	CNVD-2014-04205	D-link DWR-113 Wireless Router 跨站请求伪造漏洞	低	是
电信	CNVD-2014-04210	SYAC TB DigiEye 3G 产品后门未授权访问漏洞	高	否
电信	CNVD-2014-04227	Cisco IOS 和 IOS XE 软件存在 NTP 访问组漏洞	中	是
电信	CNVD-2014-04222	Cisco Series IP Phones 存在未明跨站脚本漏洞	中	是
电信	CNVD-2014-04221	Cisco Small Business Series IP Phones 代码执行漏洞	中	是
移动互联网	CNVD-2014-04225	Google Android 'ContactsListActivity.java'远程安全绕过漏洞	中	是
移动互联网	CNVD-2014-04224	Google Android 拨打权限绕过漏洞	中	是
移动互联网	CNVD-2014-04223	Google Android 开发桥接授权安全绕过漏洞	中	是
工控系统	CNVD-2014-04231	Yokogawa 多个产品 'BKFSim_vhfd.exe' 缓冲区溢出漏洞	高	否

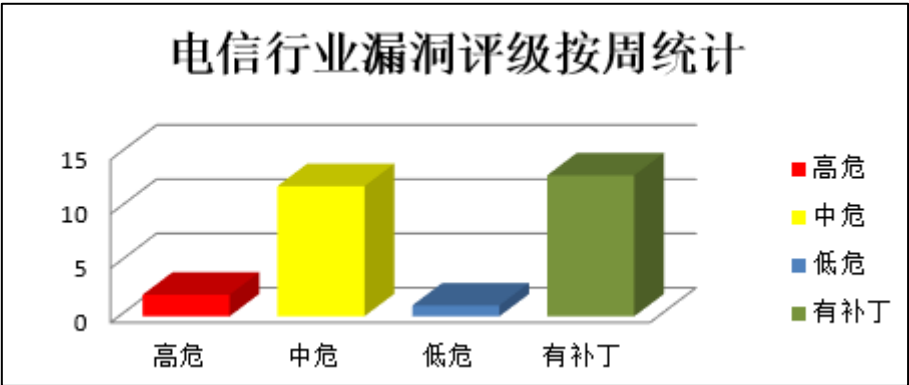


图 1 电信行业漏洞统计

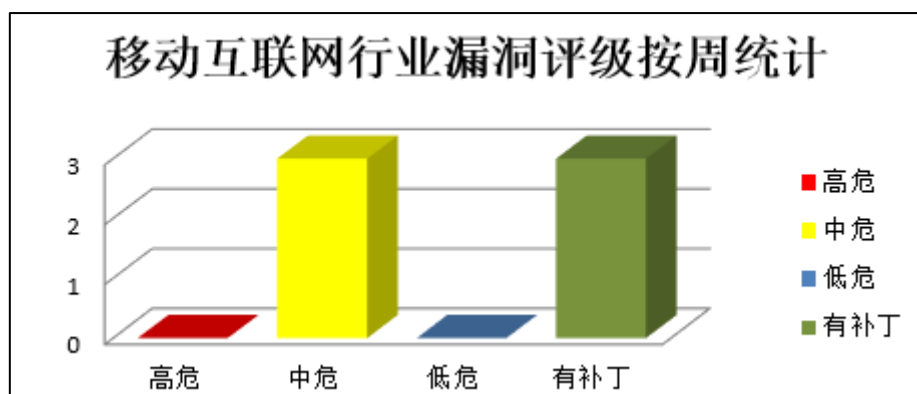


图 2 移动互联网行业漏洞统计

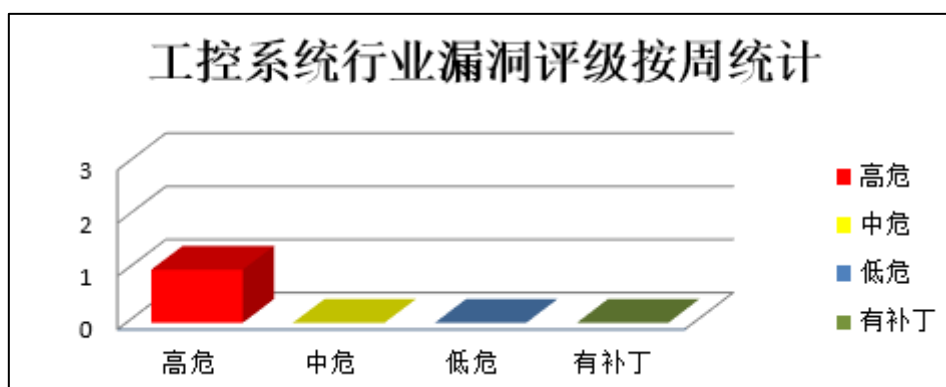


图 3 工控系统行业漏洞统计

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

7 月 9 日，微软发布了 2014 年 7 月份的月度例行安全公告，共含 6 项更新，修复了 Microsoft Windows、Internet Explorer 和 Service Bus for Windows Server 中存在的 29 个安全漏洞。其中，2 项更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可以执行任意代码，提升权限，发起拒绝服务攻击。CNVD 提醒广大 Microsoft 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。

CNVD 收录的相关漏洞包括：Microsoft Internet Explorer 存在未明内存破坏漏洞（CNVD-2014-04247、CNVD-2014-04234、CNVD-2014-04235、CNVD-2014-04237、CNVD-2014-04236）。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/webinfo/show/3467>

2、Cisco 产品安全漏洞

Cisco Unified Communications Manager 是一款 Cisco IP 电话解决方案中的呼叫处理组件。Cisco IOS 是多数思科系统路由器和网络交换机上使用的互联网络操作系统。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞绕过权限执行未授权操作或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Unified Communications Domain Manager BV SMWeb 安全绕过漏洞、Cisco Unified Communications Domain Manager 未授权访问漏洞（CNVD-2014-04106）、Cisco Unified Communications Domain Manager 特权提升漏洞、Cisco IOS 和 IOS XE 软件存在 NTP 访问组漏洞、Cisco IOS XR Software Static Punt Policer 拒绝服务漏洞。其中，除“Cisco IOS 和 IOS XE 软件存在 NTP 访问组漏洞、Cisco IOS XR Software Static Punt Policer 拒绝服务漏洞”外，其余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-2014-04105>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04106>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04107>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04227>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04083>

3、HP 产品安全漏洞

HP Universal CMDB（配置管理数据库）是美国惠普（HP）公司的一套可存储、控制并管理软件和基础设施的组件及其相互关系的数据库软件。HP SiteScope 是美国惠普（HP）公司的一套应用监控解决方案。本周，上述产品被披露存在未明漏洞和验证绕过漏洞，攻击者可利用漏洞绕过身份验证、获取敏感信息或执行任意代码。

CNVD 收录的相关漏洞包括：HP Universal CMDB 存在未明漏洞（CNVD-2014-04139、CNVD-2014-04138、CNVD-2014-04140）、HP SiteScope 验证绕过漏洞。上述漏洞的综合评级为“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-2014-04139>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04138>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04140>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04141>

4、Linux 产品安全漏洞

Linux kernel 是一款开源的操作系统。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或使应用程序崩溃，导致拒绝服务。

CNVD 收录的相关漏洞包括：Linux kernel ALSA control sound/core/control.c 内存错误引用漏洞、Linux kernel ALSA control snd_ctl_elem_user_tlv 信息泄露漏洞、Linux

kernel ALSA control 存在多个整数溢出漏洞、Linux kernel ALSA control snd_ctl_elem_add 整数溢出漏洞。其中“Linux kernel ALSA control sound/core/control.c 内存错误引用漏洞、Linux kernel ALSA control snd_ctl_elem_user_tlv 信息泄露漏洞”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-2014-04202>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04201>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04204>
<http://www.cnvd.org.cn/flaw/show/CNVD-2014-04203>

5、Dolibarr 存在多个漏洞

Dolibarr CMS 是一款内容管理系统。本周，Dolibarr CMS 被披露存在综合评级为“高危”的多个安全漏洞。攻击者可以利用漏洞获取敏感信息，劫持会话，执行任意代码等。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-2014-04226>

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-2014-04093	openSIS 'index.php'存在多个 SQL 注入漏洞	高	暂无
CNVD-2014-04099	Ruby on Rails 'ActiveRecord' SQL 注入漏洞（CNVD-2014-04099）	高	Ruby on Rails 3.2.19, 4.0.7 & 4.1.3 已经修复该漏洞，建议用户下载更新： http://www.rubyonrails.com/
CNVD-2014-04084	HylaFAX+ USER Command 远程堆缓冲区溢出漏洞	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://hylafax.sourceforge.net/
CNVD-2014-04082	RealPlayer mp4 文件原子处理内存破坏漏洞	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://service.real.com/realplayer/security/06272014_player/en/
CNVD-2014-04102	OpenStack Keystone Trust 特权提升漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： https://bugs.launchpad.net/keystone/+bug/1331912

CNVD-2014-04100	Ruby on Rails 'ActiveRecord' SQL 注入漏洞	高	Ruby on Rails 3.2.19、4.0.7 & 4.1.3 已经修复该漏洞，建议用户下载更新： http://www.rubyonrails.com/
CNVD-2014-04130	Yii PHP Framework 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，补丁获取链接： http://www.yiiframework.com/news/78/yii-1-1-15-is-released-security-fix/
CNVD-2014-04145	Apache Syncope 不安全密码生成漏洞	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://svn.apache.org/viewvc?view=revision&revision=1596537 http://syncope.apache.org/security.html
CNVD-2014-04137	Autodesk VRED Professional 2014 Python API 访问远程代码执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://www.autodesk.com/products/vred/overview
CNVD-2014-04155	NetIQ Security Manager 目录遍历漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： https://www.netiq.com/support/kb/doc.php?id=7015309

表 3 部分高危漏洞列表

小结：本周，微软发布了 2014 年 7 月份的月度例行安全公告，共含 6 项更新，修复了 Microsoft Windows、Internet Explorer 和 Service Bus for Windows Server 中存在的 29 个安全漏洞。其中，2 项更新的综合评级为最高级“严重”级别。此外，Cisco、HP、Linux 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授权操作。另外，Dolibarr CMS 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，劫持会话，执行任意代码等。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、Adobe 修补 Flash Player / AIR 产品漏洞

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, Adobe 修补了上述产品存在的安全绕过和跨站请求伪造漏洞, 避免远程攻击者利用漏洞构建恶意 WEB, 诱使用户解析, 可绕过安全限制执行恶意操作。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/47383>

<http://www.cnvd.org.cn/patchInfo/show/47380>

<http://www.cnvd.org.cn/patchInfo/show/47264>



本周要闻速递

1. Flash 严重漏洞波及多个网站

谷歌信息安全工程师米歇尔·斯帕格鲁诺(Michele Spagnuolo)周二表示: 一种与 Adobe Flash 文件有关的攻击方式正导致数百万用户的身份认证信息面临风险, 而涉及的网站和服务包括: eBay、Tumblr 和 Instagram。通过这种攻击方式, 攻击者可以在 Flash 文件中植入恶意命令。目前, 针对这一安全威胁, Adobe 已于周二发布补丁。但是, 终端用户安装这一补丁的过程可能需要几天至几周, 因此, 研究人员建议, 大型网站的工程师可以在服务器一侧进行调整, 以降低风险。

参考链接: <http://safe.zol.com.cn/465/4657574.html>

2. Android 暴露严重安全漏洞

近期 Android 系统中出现一全新漏洞, 可让有心人士透过恶意软件任意拨打使用者电话, 导致用户产生额外的通话费用, 造成严重经济损失。此漏洞影响范围包括 Android 4.1 以及 Android 4.2 的大部分用户, 全球预计有超过 59% 使用者将受到该漏洞的危害。一般在 Android 系统中, 必须申请拨打电话权限的应用程序, 才能拨打电话。但在系统应用 “Phone” 中存在的重大漏洞, 导致各种应用都能在没有权限的情形下, 随意拨打用户的电话、挂断电话, 甚至发送 USSD/SS/MMI 指令, 这将导致用户的 SIM 卡锁死、手机资料遭清除等等后果, 对使用者造成巨大损害。

参考链接: <http://tech.hexun.com/2014-07-12/166558651.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