

信息安全漏洞周报

2014 年 6 月 23 日-2014 年 6 月 29 日

2014 年第 26 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 122 个，其中高危漏洞 24 个、中危漏洞 79 个、低危漏洞 19 个。上述漏洞中，可利用来实施远程攻击的漏洞有 101 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“Zeus Cart 'prodid' SQL 注入漏洞”，“FreeFloat FTP Server 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 7 家成员单位、合作伙伴及个人报送了本周收录的全部 122 个漏洞。报送情况如表 1 所示。其中，奇虎 360、安天实验室、恒安嘉新、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、High-Tech Bridge Security Research 及白帽子向 CNVD 提交了 164 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	93	93
安天实验室	84	0
恒安嘉新	80	0
启明星辰	72	0
天融信	64	0
绿盟科技	33	0
东软	2	0

习科网络安全	17	17
CNCERT 江西分中心	15	15
CNCERT 山东分中心	13	13
CNCERT 山西分中心	10	10
CNCERT 福建分中心	7	7
CNCERT 湖南分中心	3	3
CNCERT 湖北分中心	2	2
CNCERT 宁夏分中心	2	2
High-Tech Bridge Security Research	1	1
个人	1	1
报送总计	499	164
录入总计	122（去重）	164

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、Linux、Drupal 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	7	6%
2	Linux	6	5%
3	Drupal	5	4%
4	ZTE	4	3%
5	IBM	4	3%
6	Microsoft	3	2%
7	HP	3	2%
8	Cisco	2	2%
9	D-Link	2	2%
10	其他	86	71%

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 122 个漏洞。其中应用程序漏洞 61 个，WEB 应用漏洞 33 个，网络设备漏洞 14 个，操作系统漏洞 10 个，安全产品漏洞 3 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	61
WEB 应用漏洞	33
网络设备漏洞	14
操作系统漏洞	10
安全产品漏洞	3
数据库漏洞	1

表 3 漏洞按影响类型统计表

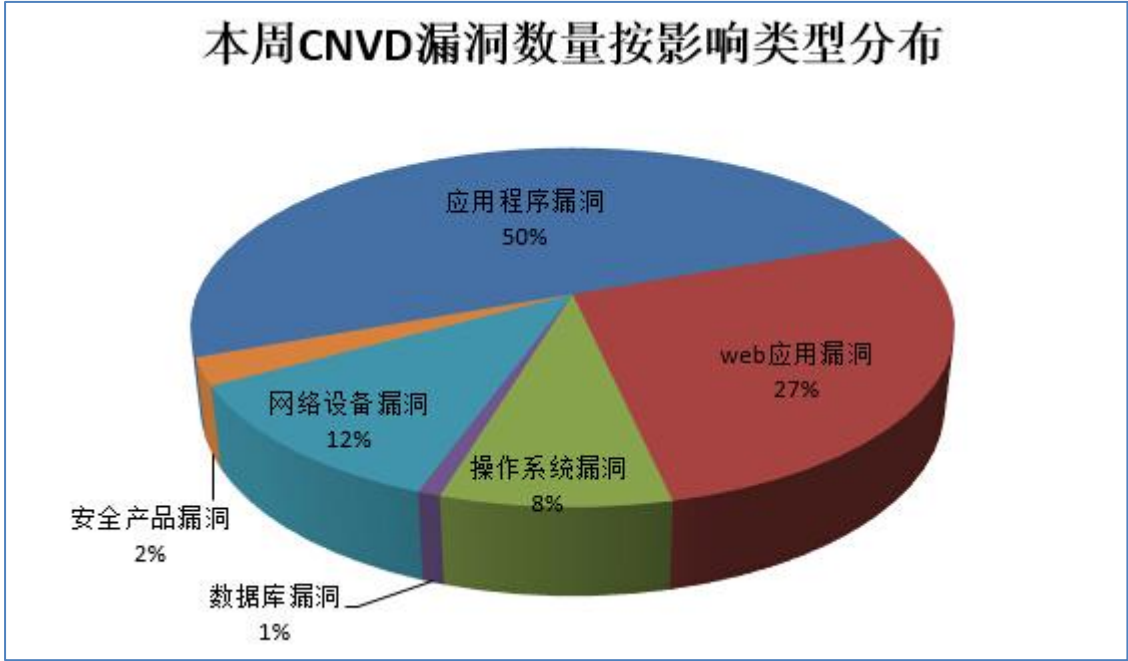


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 12 个电信行业漏洞，4 个移动互联网，1 个工控行业漏洞（如下图表所示）。其中，“Belkin N150 目录遍历漏洞”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-2014-03815	Cisco WebEx Meetings Server 信息泄露漏洞（CNVD-2014-03815）	中	是
电信	CNVD-2014-03817	Belkin N150 目录遍历漏洞	高	是
电信	CNVD-2014-03819	ZTE ZXV10 W300 Router '/basic/home_wan.htm' 框架源码泄露漏洞	高	否
电信	CNVD-2014-03841	ZTE WXV10 W300 跨站请求伪造漏洞	中	是
电信	CNVD-2014-03842	ZTE WXV10 W300 默认密码漏洞	中	是
电信	CNVD-2014-03843	ZTE WXV10 W300 备份文件泄露漏洞	中	是
电信	CNVD-2014-03867	D-Link DSL-2760U-E1 路由器'dhcpinfo.	中	否

		html' HTML 注入漏洞		
电信	CNVD-2014-03873	Motorola SBG901 跨站请求伪造漏洞	中	是
电信	CNVD-2014-03891	多个 Sitecom 产品 Admin 密码密钥安全限制绕过漏洞	低	否
电信	CNVD-2014-03881	Cisco IOS Malformed IPsec 包处理远程拒绝服务漏洞	中	是
电信	CNVD-2014-03917	ZyXEL P660RT2 EE 存在多个漏洞	中	否
电信	CNVD-2014-03922	D-link DSL-2760U-E1 跨站点脚本漏洞	中	是
移动互联网	CNVD-2014-03848	JR East Japan for Android SSL 证书验证安全绕过漏洞	中	是
移动互联网	CNVD-2014-03890	Nokia Symbian 硬编码加密密钥漏洞	中	否
移动互联网	CNVD-2014-03887	Paypal for Android 远程任意代码执行漏洞	高	否
移动互联网	CNVD-2014-03900	Android KeyStore Service 栈缓冲区溢出漏洞	中	是
工控系统	CNVD-2014-03822	MODICON M218 PLC 非法指令拒绝服务漏洞	高	否

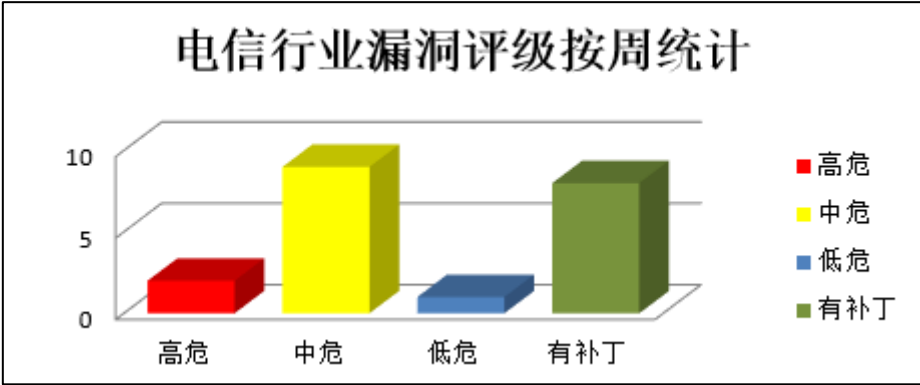


图 1 电信行业漏洞统计

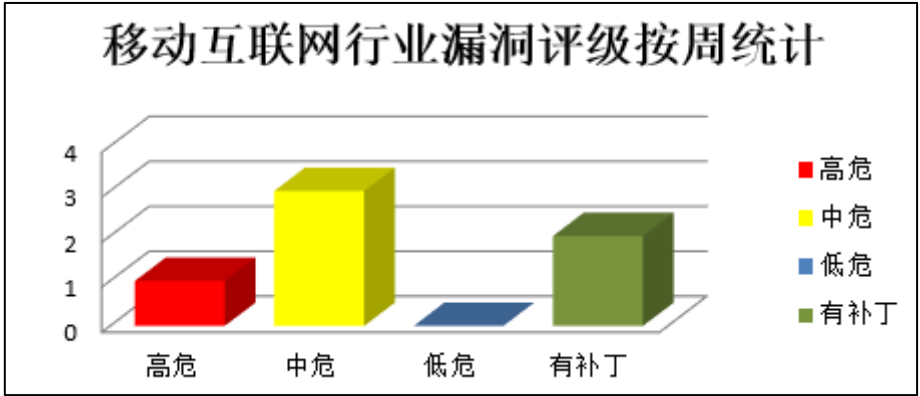


图 2 移动互联网行业漏洞统计

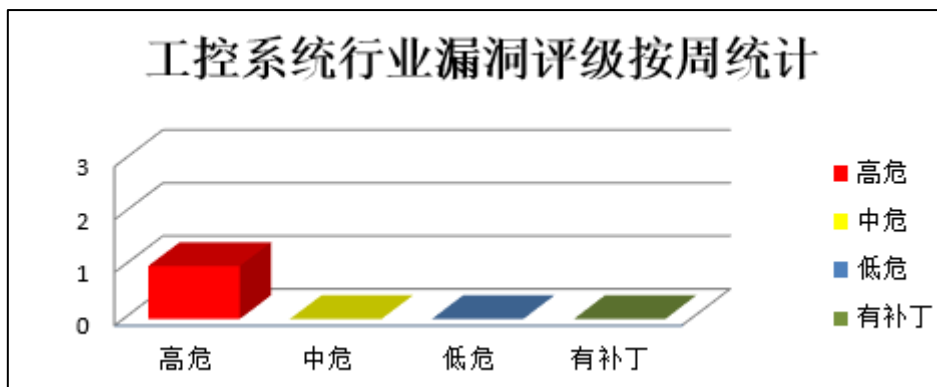


图3 工控行业漏洞统计

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、HP 产品安全漏洞

HP IT Executive Scorecard 是一个 IT 绩效管理解决方案。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞提交特殊的请求执行任意代码。

CNVD 收录的相关漏洞包括：HP Executive Scorecard 远程代码执行漏洞（CNVD-2014-03911、CNVD-2014-03912）、HP Executive Scorecard 存在多个未明远程代码执行漏洞。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-2014-03911>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03912>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03851>

2、IBM 产品安全漏洞

IBM Security Access Manager 软件是可扩展的用户认证、授权和 Web SSO 解决方案,用于在各种 Web 和应用资源上实施安全策略,集中管理在线门户网站。IBM System Storage Storwize V7000 Unified 是美国 IBM 公司的一套 Storwize 系列中的专为中小企业设计的增强版虚拟化存储系统。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、进行未授权操作或执行任意代码。

CNVD 收录的相关漏洞包括：IBM Security Access Manager for Web and Mobile 安全绕过漏洞、IBM Security Access Manager 远程代码执行漏洞、IBM Security Access Manager 安全绕过漏洞、多个 IBM 产品未授权访问漏洞。其中“IBM Security Access Manager for Web and Mobile 安全绕过漏洞、IBM Security Access Manager 远程代码执行漏洞”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-2014-03856>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03857>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03855>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03832>

3、ZTE 产品安全漏洞

ZTE ZXV10 W300 Router 是中国中兴通讯 (ZTE) 公司的一款无线路由器产品。ZTE WXV10 W300 是一款无线路由器设备。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执行未授权访问。

CNVD 收录的相关漏洞包括: ZTE ZXV10 W300 Router '/basic/home_wan.htm' 框架源码泄露漏洞、ZTE WXV10 W300 跨站请求伪造漏洞、ZTE WXV10 W300 默认密码漏洞、ZTE WXV10 W300 备份文件泄露漏洞。其中“ZTE ZXV10 W300 Router '/basic/home_wan.htm' 框架源码泄露漏洞”的综合评级为“高危”。目前, 除“ZTE ZXV10 W300 Router '/basic/home_wan.htm' 框架源码泄露漏洞”外, 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-2014-03819>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03841>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03842>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03843>

4、Drupal 产品安全漏洞

Drupal 是一套开放源码的内容管理平台。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安全限制、执行未授权操作或进行跨站脚本攻击。

CNVD 收录的相关漏洞包括: Drupal Password Policy 模块安全绕过漏洞、Drupal Password Policy 模块存在多个漏洞、Drupal Custom Meta 模块存在多个跨站脚本漏洞、Drupal Course 模块访问绕过漏洞、Drupal Easy Breadcrumb 模块存在未明跨站脚本漏洞。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-2014-03875>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03876>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03877>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03878>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03869>

5、ZeroCMS 'zero_transact_user.php' SQL 注入漏洞

ZeroCMS 是一个内容管理系统。本周, ZeroCMS 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可以利用漏洞访问或修改数据库数据。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/flaw/show/CNVD-2014-03827>

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/flare/list.htm>

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2014-03824	CTDB 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: https://ctdb.samba.org/
CNVD-2014-03838	WebminUsermin 远程命令注入漏洞	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.webmin.com/webmin/
CNVD-2014-03831	Red Hat OpenShift Enterprise 'rubygem-openshift-origin-node'远程命令执行漏洞	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: https://rhn.redhat.com/errata/RHSA-2014-0762.html
CNVD-2014-03830	Foreman Smart-Proxy 远程命令注入漏洞	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://projects.theforeman.org/issues/6086
CNVD-2014-03845	UbisoftRayman Legends 'memset()'函数栈缓冲区溢出漏洞	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.ubi.com/UK/
CNVD-2014-03852	FreeFloat FTP Server 缓冲区溢出漏洞	高	暂无
CNVD-2014-03861	Apache Shiro 'login.jsp'安全绕过漏洞	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://shiro.apache.org/
CNVD-2014-03892	X2CRM 'ProfileController.php'任意文件上传漏洞	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://x2community.com/
CNVD-2014-03902	JBoss Seam 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://www.jboss.org/
CNVD-2014-03919	Lunar CMS 'connector.php'存在多个远程命令执行漏洞	高	用户可联系厂商获得相应的升级或补丁程序: http://lunarcms.com/Get.html

表 3 部分高危漏洞列表

小结：本周，HP 产品被披露存在多个漏洞，攻击者可利用漏洞提交特殊的请求执行任意代码。此外，IBM、ZET、Drupal 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，ZeroCMS 被披露存在一个高危零日漏洞。攻击者可以利用漏洞访问或修改数据库数据。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、Microsoft 修补 Internet Explorer 产品漏洞

Internet Explorer 是微软公司推出的一款网页浏览器。

本周，Microsoft 修补了上述产品存在的内存破坏漏洞，避免攻击者通过特制的网站，利用此漏洞可执行任意代码或造成拒绝服务。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/46628>

本周要闻速递

1. iOS 系统 SSL 漏洞卷土重来

6 月 25 日消息，安全研究人员提前在 iOS 的 SSL 安全加密认证中发现了一个代码错误，它可绕过安全通信网络协议中的关键认证步骤。通过无安全保障的 Wi-Fi 热点发送的信息在未经加密的情况下，很容易被攻击者拦截，从而暴露用户的个人密码、银行数据以及其他敏感信息。

参考链接：<http://iphone.265g.com/news/146519.html>

2. TP-Link 发紧急公告：警惕“路由器安全免费软件”

近日，不少“路由器安全免费软件”现身网络。TP-Link 表示，路由器管理员密码，如同银行卡密码一样，在任何情况下都不要将其提供给任何第三方人员和机构！一旦用户将路由器管理密码输入到这类“安全软件”中，就意味着将自己路由器的管理权限完全交给了对方！这类“安全软件”将获得路由器的管理权限，就可能会控制路由器、监视用户上网行为，您的任何上网行为和相关数据，都可能暴露给对方，包括网银/网购帐号的密码、信用卡网络支付信息等等，很可能造成您的财产损失和上网隐私泄露！

参考链接：<http://digi.163.com/14/0630/05/9VVBVBDQ00162DSP.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