

信息安全漏洞周报

2013 年 07 月 22 日-2013 年 07 月 28 日

2013 年第 30 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 143 个，其中高危漏洞 42 个、中危漏洞 88 个、低危漏洞 13 个。上述漏洞中，可利用来实施远程攻击的漏洞有 130 个。本周收录的漏洞中，已有 104 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“YardRadius src/log.c 消息记录格式串漏洞”、“MLM SQL 注入漏洞”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 家成员单位及个人报送了本周收录的全部 143 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、安天实验室、天融信等单位报送数量较多。此外，知道创宇公司、High-TechBridge Security Research Lab 以及个人报送者向 CNVD 提交了 24 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	102	0
绿盟科技	28	0
安天实验室	78	0
天融信	61	0
恒安嘉新	29	0
知道创宇	2	2
东软	6	0

High-Tech Bridge	2	2
个人	20	20
报送总计	329	24
录入总计	143（去重）	24

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cisco、IBM、HP 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	Cisco	13	9%
2	IBM	11	8%
3	HP	11	8%
4	WordPress	7	5%
5	McAfee	5	3%
6	Best Practical Solutions	4	3%
7	Drupal	4	3%
8	Linux	3	2%
9	Apache	3	2%
10	Dell	3	2%
11	其它	79	55%

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 143 个漏洞。其中应用程序漏洞 87 个，WEB 应用漏洞 36 个，操作系统漏洞 3 个，网络设备漏洞 11 个，安全产品漏洞 6 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	87
WEB 应用漏洞	36
网络设备漏洞	11
操作系统漏洞	3
安全产品漏洞	6
数据库漏洞	0

表 3 漏洞按影响类型统计表

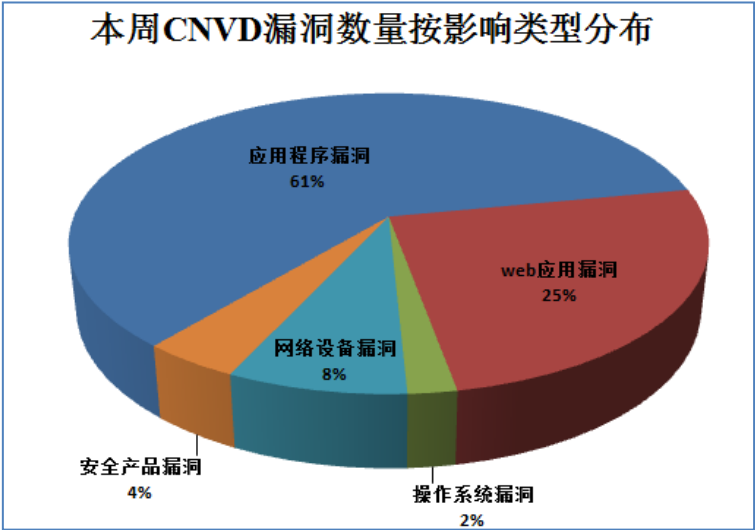


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 4 个电信行业漏洞（如下列表所示）。其中，“MongoDB 'conn' 远程代码执行漏洞”的综合评级为“高危”。相关厂商已经发布了漏洞修复程序。本周，CNVD 未收录移动互联网行业和工业系统行业漏洞。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-29794	Cisco Unified Operations Manager 跨站脚本漏洞（CNVD-2013-29794）	中危	有补丁
电信	CNVD-2013-29793	Cisco Unified Operations Manager HTTP 头跨站脚本漏洞	中危	有补丁
电信	CNVD-2013-29648	MongoDB 'conn'远程代码执行漏洞	高危	有补丁
电信	CNVD-2013-29643	Cisco Unified Operations Manager SQL 注入漏洞	中危	有补丁

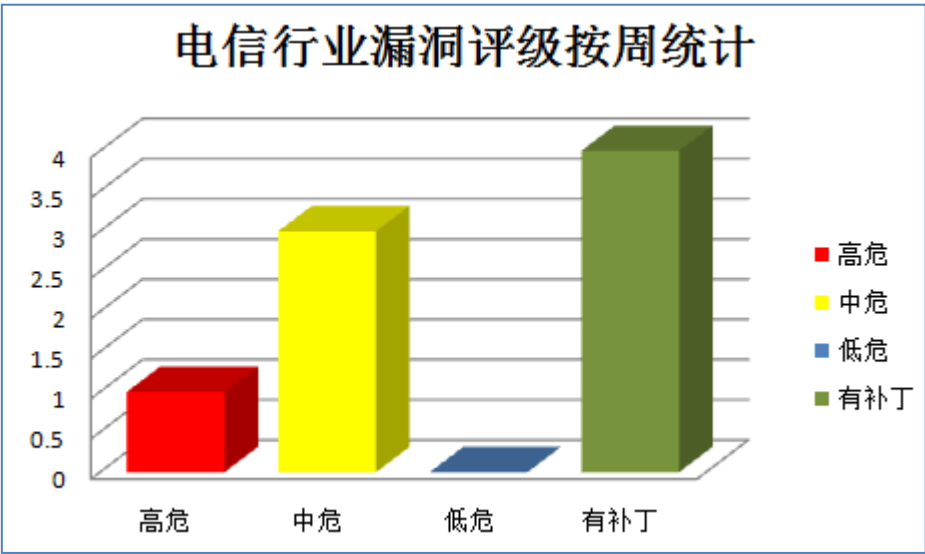


图 2 电信行业漏洞统计

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、IBM 产品安全漏洞

IBM Java 是一款 JRE 运行时环境。本周，该产品被披露存在安全漏洞，攻击者利用漏洞可远程执行任意代码。

CNVD 收录的相关漏洞包括：IBM Java 存在未明漏洞、IBM Java 存在未明任意远程代码执行漏洞（CNVD-2013-29804、CNVD-2013-29803、CNVD-2013-29802、CNVD-2013-29801、CNVD-2013-29800、CNVD-2013-29799、CNVD-2013-29798）等。上述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 提醒广大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-2013-29805>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29804>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29803>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29802>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29801>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29800>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29799>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29798>

2、Cisco 产品安全漏洞

Cisco Video Surveillance Operations Manager 是企业级视频配置和管理解决方案；Cisco Aironet 3600 access points 是一款无线接入点产品；Cisco Unified Operations Manager 是思科统一通信管理套件的组成部分，提供了基于上下文的诊断工具，以加速问题的隔离和排除；Cisco Unified IP Phones 9900 是一款 IP 电话通信设备。本周，上述思科产品被披露存在安全漏洞，远程攻击者利用漏洞可获取目标系统信息，利用这些信息获取设备的管理员控制权，访问任意文件，执行目录遍历攻击发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco Video Surveillance Manager 远程身份验证绕过漏洞（CNVD-2013-29966、CNVD-2013-29965）、Cisco Video Surveillance Manager 目录遍历漏洞、Cisco Aironet 3600 Series Access Point 远程拒绝服务漏洞、Cisco Unified Operations Manager 跨站脚本漏洞（CNVD-2013-29794）、Cisco Unified Operations Manager HTTP 头跨站脚本漏洞、Cisco Unified IP Phones 9900 Series 任意文件下载漏洞、Cisco Unified Operations Manager SQL 注入漏洞等。其中，“Cisco Video Surveillance Manager 远程身份验证绕过漏洞（CNVD-2013-29966、CNVD-2013-29965）、Cisco Video Surveillance Manager 目录遍历漏洞”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-2013-29966>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29965>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29855>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29796>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29794>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29793>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29702>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29643>

3、Apache 产品安全漏洞

Apache OFBiz 是一款开源的自动化项目系统；Apache HTTP Server 是开源 HTTP 服务器。本周，上述产品被披露存在多个安全漏洞。攻击者利用漏洞可获得敏感信息，执行任意代码。

CNVD 收录的相关漏洞包括：Apache OFBiz 嵌套表达远程代码执行漏洞、Apache OFBiz 嵌套表达远程代码执行漏洞、Apache HTTP Server 'mod_session_dbd'远程安全漏洞。其中，“Apache OFBiz 嵌套表达远程代码执行漏洞”的综合评级为“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-2013-29750>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29749>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29733>

4、Collabtive 安全漏洞

Collabtive 是一款能够协助完成项目管理的程序。本周，该产品被披露存在多个漏洞。攻击者利用漏洞可获得敏感信息，执行未经授权的操作或执行任意代码。

CNVD 收录的相关漏洞包括：Collabtive 任意文件上传漏洞、Collabtive 安全绕过漏洞（CNVD-2013-29745）、Collabtive 存在多个跨站脚本漏洞（CNVD-2013-29743）。其中，“Collabtive 任意文件上传漏洞”的综合评级为“高危”。厂商尚未发布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-2013-29744>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29745>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29743>

5、MLM SQL 注入漏洞

MLM 是一款基于 WEB 的应用程序。本周，该产品被披露存在一个综合评级为“高危”的 SQL 注入漏洞。MLM 'productview.php'脚本未能正确过滤'prdid'及'uid'参数数据，

远程攻击者利用漏洞可注入恶意 SQL 查询，获取敏感数据库信息。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-2013-29829>

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-2013-29964	vBulletin update_order 变量 SQL 注入漏洞	高	暂无
CNVD-2013-29828	Barracuda CudaTel SQL 注入漏洞	高	用户可联系厂商获得相应的升级或补丁程序： http://www.barracudanetworks.ca/cudatel.aspx
CNVD-2013-29893	Typo3 News Search ('news_search') Extension 存在未明 SQL 注入漏洞	高	暂无
CNVD-2013-29813	SurgeFTP 远程缓冲区溢出漏洞	高	SurgeFTP 23d2 已经修复此漏洞，建议用户下载更新： http://netwinsite.com/
CNVD-2013-29829	MLM SQL 注入漏洞	高	暂无
CNVD-2013-29663	Sybase EAServer 命令注入漏洞	高	用户可联系厂商获得相应的升级程序以修复此漏洞： http://www.sybase.com/downloads
CNVD-2013-29818	Photo Server 命令注入漏洞	高	暂无
CNVD-2013-29751	StatusNet 存在多个 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://status.net/2013/07/16/security-alert-sql-injection-attack-for-statusnet-1-0-x-and-1-1-x
CNVD-2013-29746	XnView PCT 文件缓冲区溢出漏洞	高	XnView v2.04 已修复此漏洞，建议用户下载使用： http://www.xnview.com/
CNVD-2013-29747	Dell Kace 1000 Systems Management Appliance 存在多个 SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结： IBM Java、Collabtiv 以及 Apache 多款产品被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息或执行任意代码。Cisco 多款产品存在的漏洞导致攻击者可获得管理员控制权，访问任意文件，执行目录遍历攻击，发起拒绝服务攻击。此外，MLM 被披露存在一个高危零日漏洞，建议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、Linux 发布升级程序，修补 Kernel 安全漏洞

Linux 是一款开源的操作系统。本周，Linux 发布升级程序，修补了 Kernel 存在的多个拒绝服务漏洞。本地和远程攻击者可利用漏洞使内核崩溃，也可能以内核权限执行任意代码。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/36388>

<http://www.cnvd.org.cn/patchInfo/show/36449>

<http://www.cnvd.org.cn/patchInfo/show/36448>

本周要闻速递

1. GPS 曝重大保安漏洞

美国最新一项研究报告指出，全球定位系统（GPS）存在重大保安漏洞，极易受到黑客和恐怖分子攻击，他们可借此劫夺邮轮和民航客机，危害极大。美国得克萨斯州大学一队研究人员使用一部手提电脑，一条小型天线和一个价值 3000 美元（约 23000 港元）的电子 GPS 干扰欺骗机，就成功控制了地中海上一艘超级游艇上的精密导航系统。

参考链接：<http://news.takungpao.com/world/exclusive/2013-07/1792659.html>

2. 利用安卓系统签名漏洞的手机木马

利用安卓系统最严重漏洞的手机木马近日频频来袭。这类使用了合法签名的木马会导致手机隐私被窃、自动向通讯录联系人群发诈骗短信以及私自发送扣费短信。某手机安全专家建议用户选择经过安全检测、可信的下载渠道下载应用，降低手机中毒风险。某手机安全中心介绍说，此前，安卓爆出史上最严重安全漏洞，安卓数字签名认证机制被攻破，黑客可在不破坏数字签名的情况下，篡改任何正常手机应用，例如植入偷帐号、窃隐私或恶意扣费等木马程序。如今，该漏洞的危害已经显现。

参考链接：<http://mobile.163.com/13/0729/06/94UB6R0D0011671M.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

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 国际合作伙伴”关系。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999