

信息安全漏洞周报

2013 年 12 月 23 日-2013 年 12 月 29 日

2013 年第 52 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 117 个，其中高危漏洞 28 个、中危漏洞 71 个、低危漏洞 18 个。上述漏洞中，可利用来实施远程攻击的漏洞有 105 个。本周收录的漏洞中，已有 93 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“EtoShop Dynamic Biz Website Builder (QuickWeb) 存在多个 SQL 注入漏洞”、“phpMyRecipes 存在多个远程漏洞”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 8 家成员单位、合作伙伴、国家互联网应急中心和分中心及个人报送了本周收录的全部 117 个漏洞。报送情况如表 1 所示。其中，安天实验室、天融信、启明星辰等单位报送数量较多。此外，国家互联网应急中心和分中心、High-Tech Bridge Security Research Lab、上海交大及个人报送者向 CNVD 提交了 42 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	114	0
天融信	75	0
启明星辰	44	0
绿盟	27	0
恒安嘉新	20	0
知道创宇	3	1

东软	3	0
奇虎 360	1	0
国家互联网应急中心	1	1
各省分中心	31	31
High-Tech Bridge Security Research Lab	3	3
上海交大	1	1
个人	5	5
报送总计	328	42
录入总计	117（去重）	42

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 IBM.、D-Link、Cisco 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	IBM	15	13%
2	D-Link	8	7%
3	Cisco	5	4%
4	TYPO3	5	4%
5	Open Text Corporation	5	4%
6	Google	4	3%
7	Wordpress	4	3%
8	FFmpeg	4	3%
9	Red Hat	1	1%
10	其它	66	58%

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 117 个漏洞。其中应用程序漏洞 81 个，WEB 应用漏洞 21 个，操作系统漏洞 3 个，网络设备漏洞 12 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	81
WEB 应用漏洞	21
网络设备漏洞	12
操作系统漏洞	3

安全产品漏洞	0
数据库漏洞	0

表 3 漏洞按影响类型统计表

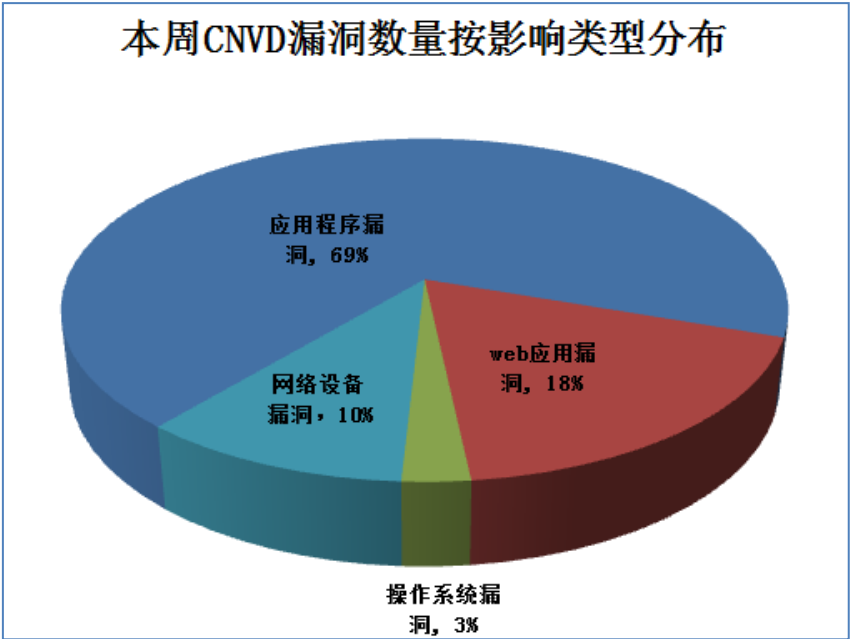


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 17 个电信行业漏洞、1 个移动互联网行业漏洞和 4 个工控系统漏洞（如下列表所示）。其中，“D-Link DSR 路由器内置账户漏洞、D-Link DIR-645 /service.cgi 特制 cookie 远程命令注入漏洞、NovaTech Orion Substation Automation Platform DNP3 驱动远程拒绝服务漏洞、General Electric (GE) Proficy HMI/SCADA - CIMPLICITY gefebt.exe 远程命令执行漏洞、General Electric (GE) Proficy HMI/SCADA - CIMPLICITY WebView 存在未明远程命令执行漏洞”的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-15507	D-Link DSR Router Series 帐户凭据存在多个信息泄露漏洞	中	是
电信	CNVD-2013-15518	Cisco NX-OS Command Line Interface (CLI)本地任意文件访问漏洞	中	否
电信	CNVD-2013-15528	IBM WebSphere Portal 内容模版目录远程代码执行漏洞	低	是
电信	CNVD-2013-15527	IBM WebSphere Portal WEB 内容管理程序信息泄露漏洞	中	是
电信	CNVD-2013-15526	IBM WebSphere Portal WCM 跨站脚本	中	是

		漏洞		
电信	CNVD-2013-15525	IBM WebSphere Portal 信息泄露漏洞	中	是
电信	CNVD-2013-15524	IBM WebSphere Portal 远程信息泄露漏洞	中	是
电信	CNVD-2013-15548	D-Link DSR 路由器内置账户漏洞	高	是
电信	CNVD-2013-15551	D-Link DIR-645 Widget 验证未授权访问漏洞	中	是
电信	CNVD-2013-15550	D-Link DIR-645 /service.cgi 特制 cookie 远程命令注入漏洞	高	是
电信	CNVD-2013-15557	Cisco EPC3925 'DdnsHostName' HTML 注入漏洞	中	否
电信	CNVD-2013-15558	Cisco IOS XE telnet 验证绕过漏洞	中	是
电信	CNVD-2013-15556	D-Link DIR-645 getfile API 路径遍历任意文件访问漏洞	中	是
电信	CNVD-2013-15555	D-Link DIR-645 version.php 验证绕过远程信息泄露漏洞	中	是
电信	CNVD-2013-15554	D-Link DIR-645 router_info.xml 远程信息泄露漏洞	中	是
电信	CNVD-2013-15553	D-Link DIR-645 '__ajax_explorer.sgi'验证绕过漏洞	中	是
电信	CNVD-2013-15580	Cisco IOS XE Software MPLS IP 分片拒绝服务漏洞	中	是
移动互联网	CNVD-2013-15490	Tube Map Live Underground for Android Oyster 信息泄露漏洞	中	是
工控系统	CNVD-2013-15486	NovaTech Orion Substation Automation Platform DNP3 驱动远程拒绝服务漏洞	高	是
工控系统	CNVD-2013-15487	NovaTech Orion Substation Automation Platform DNP3 驱动本地拒绝服务漏洞	中	是
工控系统	CNVD-2013-15501	General Electric (GE) Proficy HMI/SCADA - CIMPLICITY gefebt.exe 远程命令执行漏洞	高	是
工控系统	CNVD-2013-15504	General Electric (GE) Proficy HMI/SCADA - CIMPLICITY WebView 存在未明远程命令执行漏洞	高	是

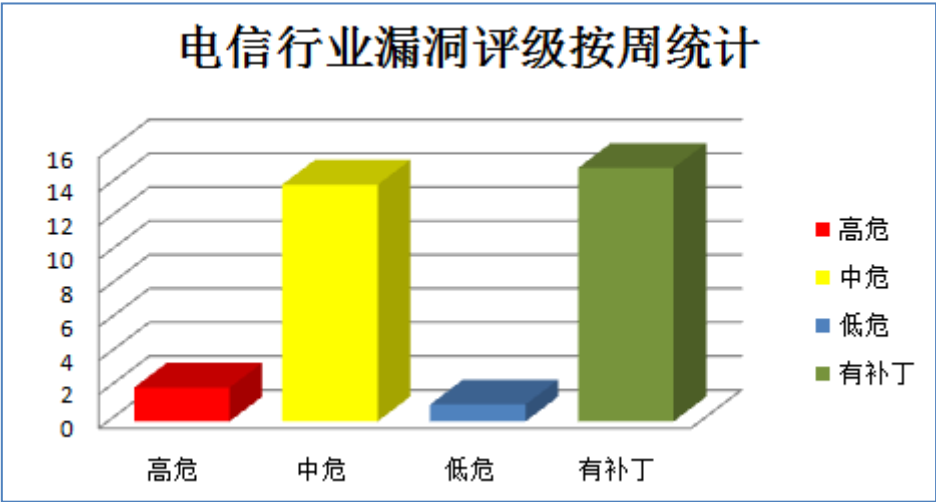


图 1 电信行业漏洞统计

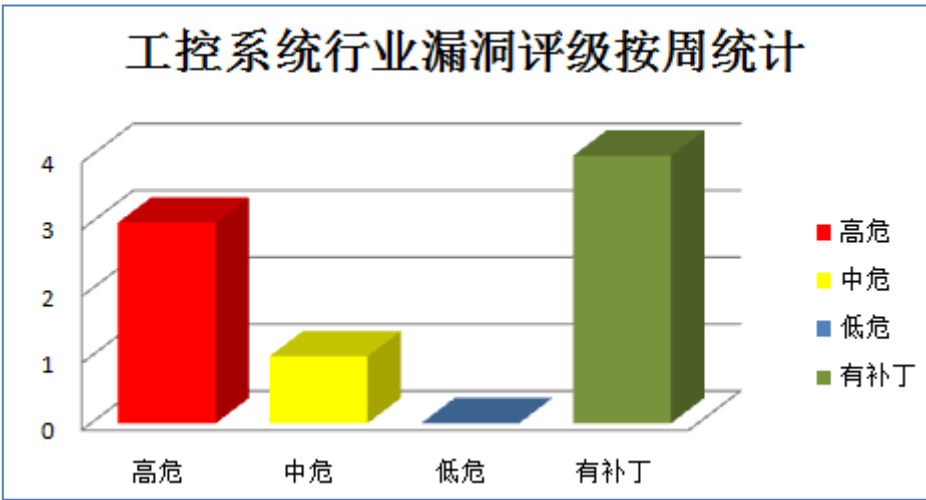


图 2 工控系统行业漏洞统计

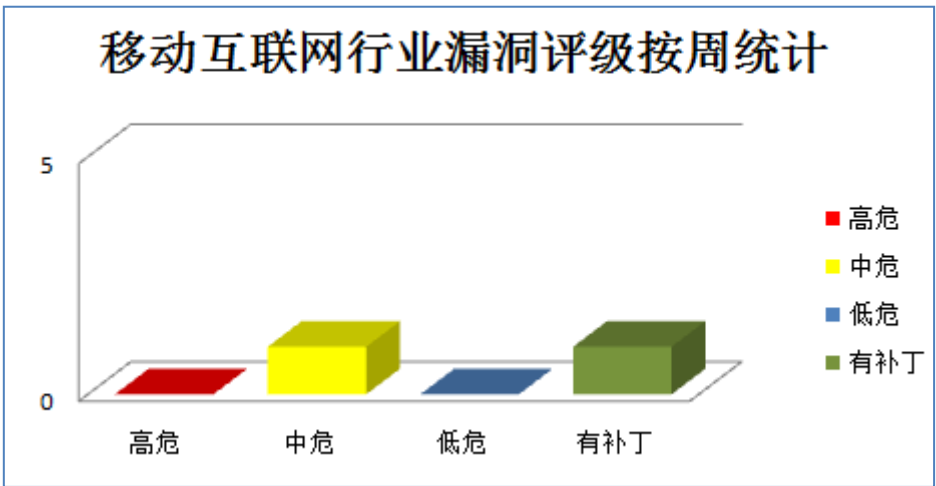


图 3 移动互联网行业漏洞统计

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Google 产品安全漏洞

Picasa 是一款 Google 推出的免费图片管理工具。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Google Picasa RAW 图像文件处理远程栈缓冲区溢出漏洞、Google Picasa Canon RAW CR2 图像文件 JPEG 标签处理远程堆缓冲区溢出漏洞（CNVD-2013-15544）、Google Picasa Canon RAW CR2 图像文件 JPEG 标签处理远程堆缓冲区溢出漏洞、Google Picasa Canon RAW CR2 图像文件处理远程堆缓冲区溢出漏洞。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 提醒用户及时下载补丁更新，避免引发漏洞相关的安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15543>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15544>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15545>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15546>

2、D-Link 产品安全漏洞

D-Link DIR-645 是一款路由器设备；D-Link DSR 是无线服务路由器产品。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可绕过权限，获得敏感信息，执行任意命令。

CNVD 收录的相关漏洞包括：D-Link DIR-645 /service.cgi 特制 cookie 远程命令注入漏洞、D-Link DSR 路由器内置账户漏洞、D-Link DIR-645 Widget 验证未授权访问漏洞、D-Link DIR-645 '__ajax_explorer.sgi'验证绕过漏洞、D-Link DIR-645 router_info.xml 远程信息泄露漏洞、D-Link DIR-645 version.php 验证绕过远程信息泄露漏洞、D-Link DIR-645 getfile API 路径遍历任意文件访问漏洞、D-Link DSR Router Series 帐户凭据存在多个信息泄露漏洞。其中，“D-Link DIR-645 /service.cgi 特制 cookie 远程命令注入漏洞、D-Link DSR 路由器内置账户漏洞”的综合评级均“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安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15550>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15548>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15551>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15553>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15554>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15555>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15556>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15507>

3、IBM 产品安全漏洞

IBM WebSphere Portal 是一款基于 SOA 的解决方案；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。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。

CNVD 收录的相关漏洞包括：IBM WebSphere Portal 远程信息泄露漏洞、IBM WebSphere Portal 信息泄露漏洞、IBM WebSphere Portal WCM 跨站脚本漏洞、IBM WebSphere Portal WCM 跨站脚本漏洞、IBM WebSphere Portal 内容模版目录远程代码执行漏洞、IBM Security Access Manager for Enterprise 存在未明 HTML 注入漏洞（CNVD-2013-15529）、IBM Security Access Manager for Enterprise 存在未明 HTML 注入漏洞、IBM Security Access Manager for Enterprise 信息泄露漏洞等。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-2013-15524>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15525>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15526>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15527>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15528>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15529>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15530>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15531>

4、XnView 安全漏洞

XnView 是一款图像查看程序。本周，该产品被披露存在多个漏洞，攻击者利用漏洞可触发堆缓冲区溢出。

CNVD 收录的相关漏洞包括：XnView 存在多个缓冲区溢出漏洞（CNVD-2013-15496、CNVD-2013-15495、CNVD-2013-15494）。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-2013-15496>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15495>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15494>

5、EtoShop Dynamic Biz Website Builder (QuickWeb) 存在多个 SQL 注入漏洞

EtoShop 是一个电子商务平台。本周，EtoShop 被披露存在一个综合评级为“高危”的 SQL 注入漏洞，远程攻击者利用漏洞可对应用程序/新闻-事件/newdetailasp id 参数执行任意 SQL 命令。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-2013-15583>

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-2013-15581	iScripts AutoHoster 存在多个 SQL 注入漏洞	高	暂无
CNVD-2013-15598	Synology DiskStation Manager 'imageSelector.cgi'远程命令执行漏洞	高	厂商已经发布了升级补丁, 请到厂商的主页下载: http://www.synology.com/dsm/index.php
CNVD-2013-15569	WebYaST 不安全权限特权提升漏洞	高	厂商已经发布了升级补丁, 请到厂商的主页下载: http://lists.opensuse.org/opensuse-security-announce/2013-12/msg00006.html
CNVD-2013-15566	Red Hat Subscription Asset Manager Candlepin 不安全验证方案使用漏洞	高	厂商已经发布了升级补丁, 请到厂商的主页下载: http://rhn.redhat.com/errata/RHSA-2013-1863.html
CNVD-2013-15563	phpMyRecipes 存在多个远程漏洞	高	暂无
CNVD-2013-15536	Revive Adserver 'what' SQL 注入漏洞	高	厂商已经发布了升级补丁, 请到厂商的主页下载: http://www.revive-adserver.com
CNVD-2013-15533	GOM Player '.avi'文件内存破坏漏洞	高	暂无
CNVD-2013-15540	Hancom Office HML TEXTART 标签处理堆缓冲区溢出漏洞	高	暂无
CNVD-2013-15535	Steinberg MyMp3PRO '.m3u'文件缓冲区溢出漏洞	高	暂无

表 3 部分高危漏洞列表

小结: Google Picasa、XnView 和 D-Link、IBM 的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, 导致应用程序崩溃, 执行任意代码, 或触发基于堆的缓冲区溢出。此外, EtoShop 电子商务平台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、Red Hat 修补 Subscription Asset Manager Candlepin 产品漏洞

Red Hat Subscription Asset Manager 是一款红帽推出的用于管理 RedHat 订阅的管理程序。本周，Red Hat 修补了上述产品存在的不安全验证方案使用漏洞，避免攻击者利用漏洞发起攻击。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/41999>

本周要闻速递

1. 三星 Galaxy S4 存在安全漏洞

以色列研究人员发现这款智能手机中存在一个安全漏洞，可让黑客轻易地拦截用户的数据。据悉，三星正在调查这个问题。迄今为止，该公司并不相信这个问题像以色列研究人员在其报告中所描述的那样严重。上述漏洞是以色列本古里安大学网络安全实验室的研究人员本月初发现的。他们声称，虽然 Knox 是针对手机的最先进的安全驱动型基础架构，但是它存在的漏洞可让恶意软件轻易地跟踪用户的电子邮件以及记录他们的数据通信。这个漏洞是该大学的博士生莫迪凯-古里（Mordechai Guri）在一项不相关的研究任务中发现的。

参考链接：<http://tech.qq.com/a/20131225/012875.htm>

2. ios7 越狱漏洞或被封堵

越狱团队 Evad3rs 发布的 iOS7 完美越狱工具 Evasi0n7，白苹果横行并强制捆绑了某助手，很多果粉都还在持观望态度，等待更完美的越狱工具出现。现在，苹果发话了，称在新的 ios 固件升级中，将封锁目前已经放出的越狱漏洞。近日，有消息称，苹果将会在未来的 ios 固件版本的升级推送中加入对于目前移动 4G 网络的支持，并且，还将可能封锁目前已经放出的越狱漏洞。

参考链接：http://www.25pp.com/news/news_55376.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