

信息安全漏洞周报

2013 年 08 月 05 日-2013 年 08 月 11 日

2013 年第 32 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 175 个，其中高危漏洞 67 个、中危漏洞 93 个、低危漏洞 15 个。上述漏洞中，可利用来实施远程攻击的漏洞有 160 个。本周收录的漏洞中，已有 144 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“Hikvision DS-2CD7153-E IP Camera 远程缓冲区溢出漏洞”、“Telmanik CMS Press 'page_name'参数 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 6 家成员单位和合作伙伴及个人报送了本周收录的全部 175 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、绿盟科技等单位报送数量较多。此外，知道创宇公司、上海交大、High-TechBridge Security Research Lab 以及个人报送者向 CNVD 提交了 47 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	111	0
绿盟科技	46	0
安天实验室	106	0
天融信	84	0
恒安嘉新	30	0
知道创宇	2	1

上海交大	10	10
High-Tech Bridge	3	3
个人	33	33
报送总计	425	47
录入总计	175（去重）	47

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Mozilla、Cisco、Google 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	Mozilla	15	9%
2	Cisco	12	7%
3	Google	9	5%
4	WordPress	7	4%
5	Joomla!	6	3%
6	IBM	6	3%
7	Symantec	5	3%
8	TP-Link	4	2%
9	Siemens	4	2%
10	Apache	3	1%
11	其它	104	61%

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 175 个漏洞。其中应用程序漏洞 104 个，WEB 应用漏洞 40 个，操作系统漏洞 3 个，网络设备漏洞 23 个，安全产品漏洞 5 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	104
WEB 应用漏洞	40
网络设备漏洞	23
操作系统漏洞	3
安全产品漏洞	5
数据库漏洞	0

表 3 漏洞按影响类型统计表

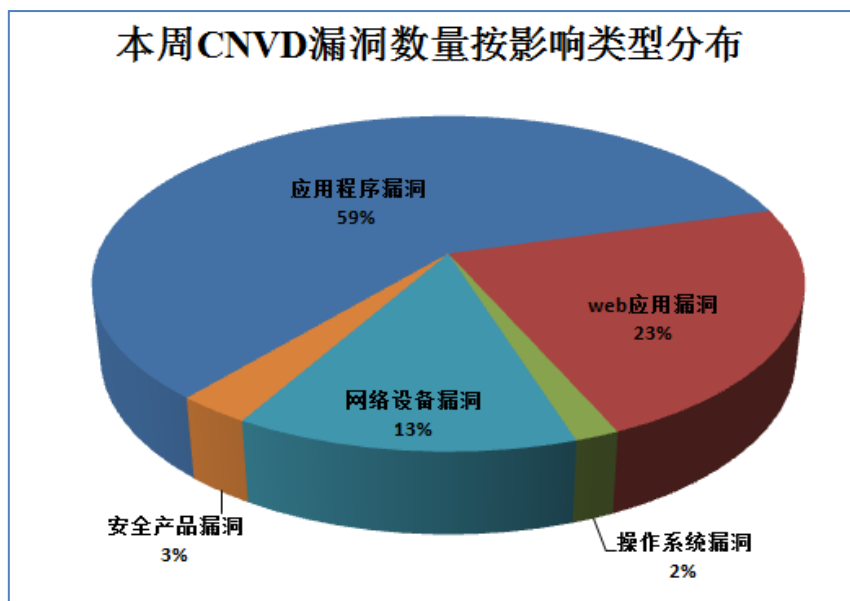


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 8 个电信行业漏洞、2 个移动互联网行业漏洞和 5 个工控系统漏洞（如下列表所示）。其中，“Vodafone EasyBox 可猜测默认 WPS-PIN 生成漏洞、D-Link DIR-645 存在多个缓冲区溢出漏洞、National Instruments Lookout ActiveX 控件存在未明漏洞、National Instruments 多个产品 cwui.ocx ActiveX 控件路径遍历漏洞、多个 IIS Server Drivers 拒绝服务漏洞”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-2013-31169	Vodafone EasyBox 可猜测默认 WPS-PIN 生成漏洞	高危	无补丁
电信	CNVD-2013-30951	MOXA OnCell Gateways 不充分熵漏洞	中危	有补丁
电信	CNVD-2013-30888	Huawei B153 3G/UMTS 路由器密码泄露访问绕过漏洞	中危	有补丁
电信	CNVD-2013-30836	D-Link DIR-645 存在多个跨站脚本漏洞	中危	有补丁
电信	CNVD-2013-30821	D-Link DIR-645 存在多个缓冲区溢出漏洞	高危	有补丁
电信	CNVD-2013-30820	Cisco WebEx Meetings Server 过期用户远程验证绕过漏洞	中危	有补丁
电信	CNVD-2013-30493	Apache Tomcat 处理远程信息泄露漏洞	中危	有补丁
电信	CNVD-2013-30466	Cisco WebEx 信息泄露漏洞	中危	有补丁
移动互	CNVD-2013-30875	Microsoft Windows Phone	中危	无补丁

联网		PEAP-MS-CHAPv2 身份验证协议漏洞		
移动互 联网	CNVD-2013-30816	Apple iOS 本地安全绕过漏洞	中危	无补丁
工控系 统	CNVD-2013-31013	National Instruments Lookout ActiveX 控件存在未明漏洞	高危	有补丁
工控系 统	CNVD-2013-31002	National Instruments 多个产品 cwui.ocx ActiveX 控件路径遍历漏洞	高危	有补丁
工控系 统	CNVD-2013-30823	多个 IOService Drivers 拒绝服务漏洞	高危	有补丁
工控系 统	CNVD-2013-30477	Siemens SIMATIC WinCC TIA Portal URL 重定向漏洞	中危	有补丁
工控系 统	CNVD-2013-30476	Siemens SIMATIC WinCC TIA Portal 跨站请求伪造漏洞	中危	有补丁

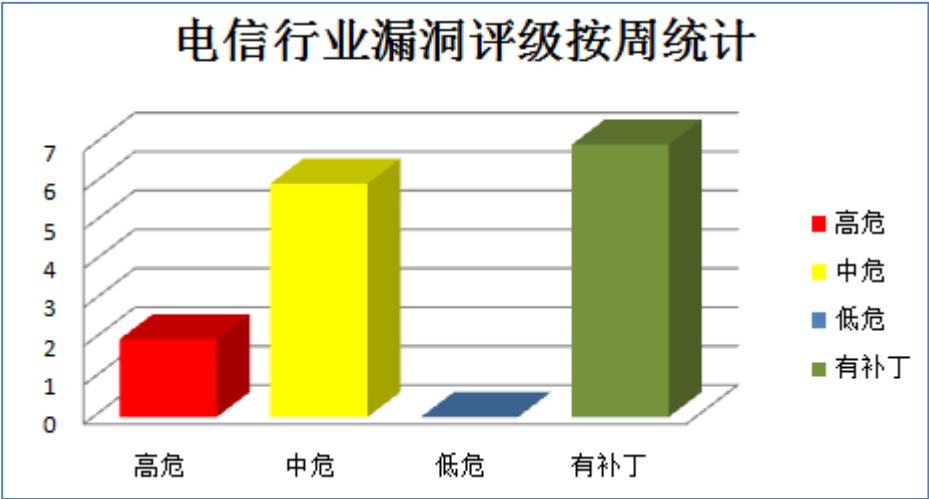


图 2 电信行业漏洞统计

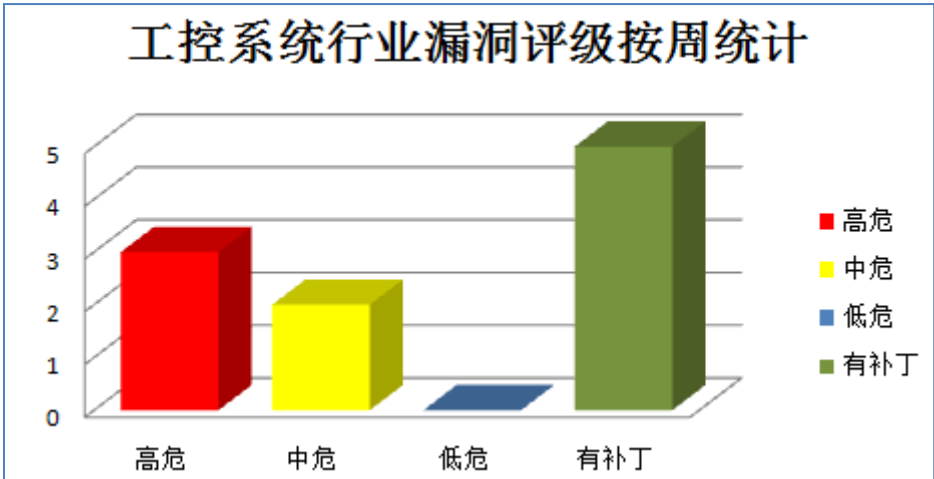


图 3 工控系统行业漏洞统计

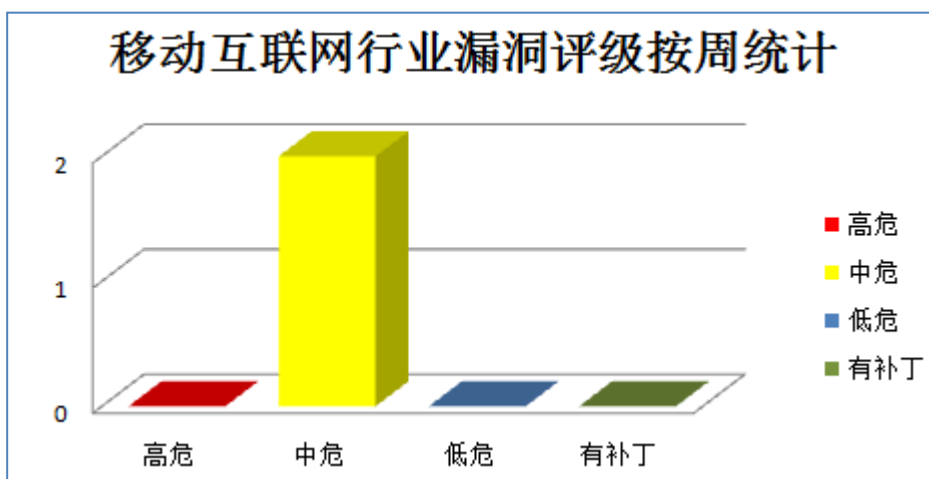


图 4 移动互联网行业漏洞统计

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、Mozilla 产品安全漏洞

Mozilla Firefox/SeaMonkey/Thunderbird 是 Mozilla 所发布的 WEB 浏览器/新闻组客户端/邮件客户端。本周，上述产品被披露存在安全漏洞，攻击者利用漏洞可导致应用程序崩溃或远程执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla 多个产品存在多个未明漏洞、Mozilla 多个产品浏览器引擎存在多个未明漏洞、Mozilla 多个产品 nsINode::GetParentNode 内存错误引用漏洞、Mozilla 多个产品 cryptojs_interpret_key_gen_type 函数堆缓冲区下溢漏洞、Mozilla 多个产品 maintenanceservice.exe 栈缓冲区溢出漏洞、Mozilla 多个产品 Mozilla Updater 栈缓冲区溢出漏洞、Mozilla 多个产品 CRMF 请求生成跨站脚本漏洞、Mozilla 多个产品不正确 URI 校验漏洞等。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-2013-30984>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30985>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30986>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30987>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30988>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30989>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30992>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30995>

2、Cisco 产品安全漏洞

Cisco TelePresence 是一款网络会议解决方案；Cisco Unified Communications Manager 是 Cisco IP 电话解决方案中的呼叫处理组件；Cisco WebEx 是一款网络会议解决方案；Cisco VC220、VC240 设备是网络摄像机。本周，上述产品被披露存在多个安全漏洞，远程攻击者利用漏洞可获得敏感信息，使设备重载，获得特权访问。

CNVD 收录的相关漏洞包括：Cisco TelePresence Web 服务器密码恢复管理账户默认验证凭据漏洞、Cisco Unified Communications Manager 跨站请求伪造漏洞、Cisco Unified Communications Manager 用户 WEB 拨号页跨站请求伪造漏洞、Cisco Unified Communications Manager 信息泄露漏洞、Cisco Unified Communications Manager 信息泄露漏洞、Cisco VC220/VC240 Network Cameras 存在多个拒绝服务漏洞。其中，“Cisco TelePresence Web 服务器密码恢复管理账户默认验证凭据漏洞”的综合评级为“高危”。厂商已发布了除“Cisco TelePresence Web 服务器密码恢复管理账户默认验证凭据漏洞”外，其余漏洞的修补程序。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-2013-31114>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30936>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30935>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30934>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30820>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30741>

3、IBM 产品安全漏洞

IBM iNotes 是一款 Web 解决方案；IBM InfoSphere BigInsights 是用于分析和虚拟化海量数据的软件。本周，上述产品被披露存在多个安全漏洞。远程攻击者利用漏洞可获得敏感信息，执行未授权的访问。

CNVD 收录的相关漏洞包括：IBM iNotes ActiveX 整数溢出漏洞、IBM iNotes 存在未明跨站脚本漏洞（CNVD-2013-31028）、IBM iNotes 存在未明跨站脚本漏洞、IBM InfoSphere BigInsights 跨站脚本漏洞、IBM InfoSphere BigInsights 跨站请求伪造漏洞、IBM InfoSphere BigInsights 任意链接注入漏洞。其中，“IBM iNotes ActiveX 整数溢出漏洞”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-2013-30945>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-31028>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30946>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30944>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30943>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-30942>

4、Hikvision 产品安全漏洞

Hikvision DS-2CD7153-E IP Camera 是一款网络摄像头产品。本周，该产品被披露存在多个漏洞，攻击者利用漏洞可使进程崩溃服务重启，绕过权限控制摄像头。

CNVD 收录的相关漏洞包括：Hikvision DS-2CD7153-E IP Camera 远程缓冲区溢出漏洞、Hikvision DS-2CD7153-E IP Camera 特权提升漏洞、Hikvision DS-2CD7153-E IP Camera 内置账户安全绕过漏洞。其中，“Hikvision DS-2CD7153-E IP Camera 远程缓冲区溢出漏洞、Hikvision DS-2CD7153-E IP Camera 特权提升漏洞”的综合评级均为“高危”。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-2013-31131>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-31130>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-31127>

5、Telmanik CMS Press 'page_name'参数 SQL 注入漏洞

Telmanik CMS Press 是一款内容管理系统。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。Telmanik CMS Press 'pages.php'脚本未能正确过滤'page_name'参数传递的输入，远程攻击者利用漏洞可注入恶意 SQL 查询，获取数据库敏感信息或控制应用系统。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-2013-30960>

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-2013-31170	Cacti SQL 注入漏洞	高	Cacti 0.8.8b 已经修复此漏洞，建议用户下载更新： http://www.cacti.net/
CNVD-2013-31169	Vodafone EasyBox 可猜测默认 WPS-PIN 生成漏洞	高	暂无
CNVD-2013-31166	PuTTY DSA 签名远程缓冲区溢出漏洞	高	PuTTY r9977 2013-07-09 0.63 已经修复此漏洞，建议用户下载更新： http://www.chiark.greenend.org.uk/~sgtatham/putty/
CNVD-2013-31159	FFmpeg/Libav vc1_decode_frame 函数非法 mb_height 处理漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： http://git.libav.org/?p=libav.git;a=commit;h=43bacd5b7d3d265a77cd29d8abb131057796aecc

			http://git.videolan.org/?p=ffmpeg.git;a=commit;h=43bacd5b7d3d265a77cd29d8abb131057796aecc
CNVD-2013-31155	Apache HTTP Server suEXEC 符号链接任意文件访问漏洞	高	暂无
CNVD-2013-31128	PuTTY 'modmul()'函数缓冲区欠载漏洞	高	PuTTY r9977 2013-07-09 0.63 已经修复此漏洞，建议用户下载更新： http://www.chiark.greenend.org.uk/~sgtatham/putty/
CNVD-2013-31125	Squash 存在多个任意代码执行漏洞	高	用户可联系供应商获得补丁信息： http://www.squashcampaign.org/
CNVD-2013-31113	phpFox 存在多个 SQL 注入漏洞	高	phpFox 3.6.0 (build6)已经修复此漏洞，建议用户下载更新： http://www.phpfox.com/
CNVD-2013-30999	National Instruments NI .NET 类库帮助 ActiveX 控件存在未明漏洞	高	用户可参考如下厂商提供的安全公告获取补丁信息： http://digital.ni.com/public.nsf/websearch/507DEC9DA57A708186257B3600512623?OpenDocument
CNVD-2013-30962	TYPO3 Faceted Search 扩展存在未明 SQL 注入漏洞	高	Faceted Search (ke_search) Extension for TYPO3 1.4.1 已经修复此漏洞，建议用户下载更新： http://typo3.org/extensions/repository/view/ke_search

表 3 部分高危漏洞列表

小结： 本周，Hikvision DS-2CD7153-E IP Camera 和 Cisco 多款产品被披露存在多个漏洞，攻击者利用漏洞可导致设备重载，提升权限。IBM 和 Mozilla 多款产品存在的漏洞可导致程序崩溃或执行未授权的操作。此外，Telmanik CMS Press 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 产品安全漏洞

Linux 是一款开源的操作系统。本周，Linux 发布升级程序，修补 Kernel 产品存在的漏洞。攻击者可利用漏洞发起拒绝服务攻击。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/38059>

本周要闻速递

1. Android 重大安全漏洞或导致比特币被窃取

北京时间 8 月 12 日早间消息，据美国科技博客 TheVerge 报道，比特币开发者近日在一篇博客中称，他们在 Android 操作系统上发现了一个重大漏洞，很容易导致比特币被黑客窃取。据悉，这一漏洞会影响每一款 Android 版比特币钱包应用，包括 Bitcoin Wallet、blockchain.info Wallet、BitcoinSpinner、Mycelium Wallet 等热门钱包应用。开发者表示，该漏洞对 Android 系统生成安全随机数字的能力带来了冲击，这些随机数字有助于用户比特币账户安全。Mt. Gox 和 Coinbase 等比特币交易平台不会受到这一漏洞的影响，因为这些服务的密钥不是在设备上随机生成的。开发者建议，那些正在使用 Android 版电子钱包应用的用户，应该用可靠的随机数生成程序生成一个新的地址，然后将所有的比特币重新放回自己的钱包中。与此同时，BitcoinTalk.org 网站上公布的信息显示，开发者计划推出一些升级，增强那些受漏洞影响的 Android 版比特币钱包应用的安全性。

参考链接：<http://tech.sina.com.cn/i/2013-08-12/09058628871.shtml>

2. iOS 存在重大漏洞据称可绕过安全机制

一直以来苹果的 iOS 就以系统的稳定与安全性著称，所以各位也因此能够很安心的使用自己的平板产品进行购物与沟通。不过佐治亚理工学院信息安全中心最近却发现了 iOS 中的重大漏洞，并公布了细节内容。据称该漏洞可以绕过苹果的安全机制，这势必会成为 iOS 平台的重大安全威胁。该漏洞允许攻击者将恶意部分隐藏起来以通过苹果的应用审核，然后在用户毫无察觉的情况下悄悄的安装在 iOS 设备中。iOS 7 已经修复了该漏洞，不过其他版本的依然存在这一问题，苹果也正在做积极的改进。

参考链接：<http://article.pchome.net/content-1642057.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