

信息安全漏洞周报

2013 年 12 月 02 日-2013 年 12 月 08 日

2013 年第 49 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 128 个，其中高危漏洞 27 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 111 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“FlashComs Chat 'file.php'任意文件上传漏洞”、“Wondershare Player 'ws_converterex.dll' dll 加载任意代码执行漏洞”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、国家互联网应急中心及个人报送了本周收录的全部 128 个漏洞。报送情况如表 1 所示。其中，安天实验室、启明星辰、天融信等单位报送数量较多。此外，国家互联网应急中心、High-Tech Bridge Security Research Lab 及个人报送者向 CNVD 提交了 11 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
启明星辰	95	0
绿盟	85	0
天融信	79	0
恒安嘉新	12	0
国家互联网应急中心	1	1
High-Tech Bridge Security Research Lab	1	1

个人	9	9
报送总计	413	11
录入总计	128（去重）	11

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Cybozu, Inc.、Cisco、Novell 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	Cybozu, Inc.	20	16%
2	Cisco	9	7%
3	Novell	7	5%
4	Ruby on Rails	5	4%
5	General Electric Company	5	4%
6	IBM	3	2%
7	Linux	3	2%
8	Apache	2	2%
9	Google	2	2%
10	其它	72	56%

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 128 个漏洞。其中应用程序漏洞 71 个，WEB 应用漏洞 38 个，操作系统漏洞 8 个，网络设备漏洞 10 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	71
WEB 应用漏洞	38
网络设备漏洞	10
操作系统漏洞	8
安全产品漏洞	1

表 3 漏洞按影响类型统计表

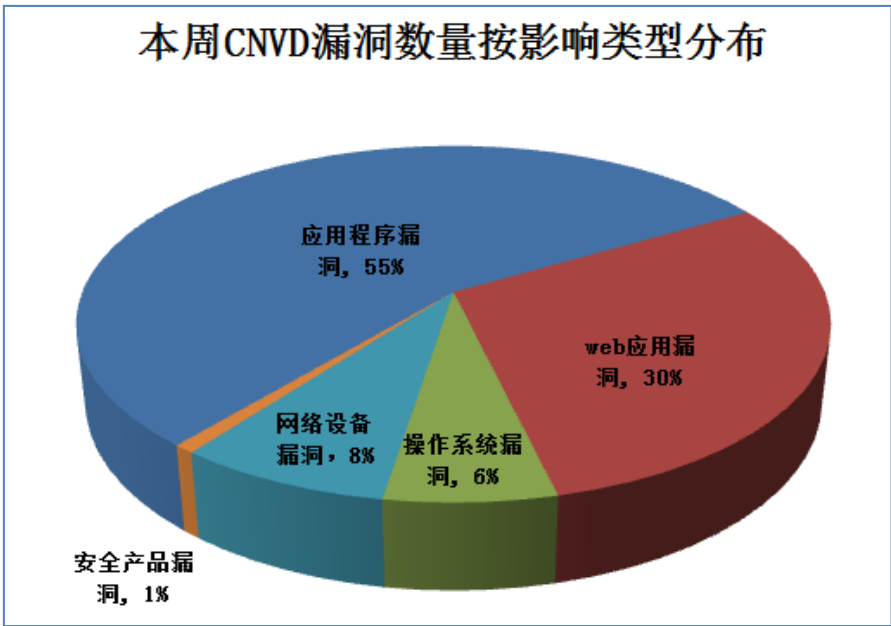


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 11 个电信行业漏洞、3 个移动互联网行业漏洞和 6 个工控系统漏洞（如下列表所示）。其中，“GE Proficy HMI/SCADA-iFIX 'TCPTASK.exe'远程缓冲区溢出漏洞、GE Proficy Machine Edition 'Trapserver.exe' 远程缓冲区溢出漏洞”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-2013-14907	ZyXEL GS1510-16 webctrl.cgi 验证绕过敏感信息获取漏洞	中	否
电信	CNVD-2013-14921	TP-Link TL-WR740N/TL-WR740ND Wireless N 路由器 HTTP 处理拒绝服务漏洞	中	否
电信	CNVD-2013-14920	Elecsys Director Gateway 拒绝服务漏洞	中	是
电信	CNVD-2013-14868	D-Link DIR 系列路由器 'model/__show_info.php'本地文件泄露漏洞	低	否
电信	CNVD-2013-14869	Cisco Prime Collaboration Assurance 跨站脚本漏洞	中	是
电信	CNVD-2013-14871	Cisco IOS Software IP Device tracking 拒绝服务漏洞	中	是
电信	CNVD-2013-14872	Cisco DPR2320R2 Wireless Router 存在多个跨站请求伪造漏洞	低	否

电信	CNVD-2013-14852	Satechi Smart Travel Router Web 管理控制台远程验证绕过漏洞	中	否
电信	CNVD-2013-14842	Cisco Secure ACS 非特权 Supoort-Bundle 下载漏洞	中	是
电信	CNVD-2013-14807	D-Link DAP-1522 无线路由器内置验证凭据安全绕过漏洞	中	否
电信	CNVD-2013-14810	Cisco IOS XE Software MPLS 报文处理远程拒绝服务漏洞	中	是
移动互联网	CNVD-2013-14828	Google Nexus Class 0 'Flash' SMS 远程拒绝服务漏洞	中	否
移动互联网	CNVD-2013-14816	LastPass For Android 本地安全绕过漏洞	中	否
移动互联网	CNVD-2013-14805	Google Android 'com.android.settings.ChooseLockGeneri c'类远程安全绕过漏洞	中	否
工控系统	CNVD-2013-14844	Alstom e-terracontrol DNP Master 驱动串口拒绝服务漏洞	中	是
工控系统	CNVD-2013-14823	GE Proficy HMI/SCADA-iFIX 'TCPTASK.exe'远程缓冲区溢出漏洞	高	是
工控系统	CNVD-2013-14825	GE Proficy HMI/SCADA-iFIX 不安全默认密码漏洞	中	是
工控系统	CNVD-2013-14824	多个 GE Proficy 产品以太网接口远程缓冲区溢出漏洞	中	是
工控系统	CNVD-2013-14826	GE Proficy HMI/SCADA-iFIX 'TCPTASK.exe'远程拒绝服务漏洞	中	是
工控系统	CNVD-2013-14827	GE Proficy Machine Edition 'Trapiserver.exe' 远程缓冲区溢出漏洞	高	是

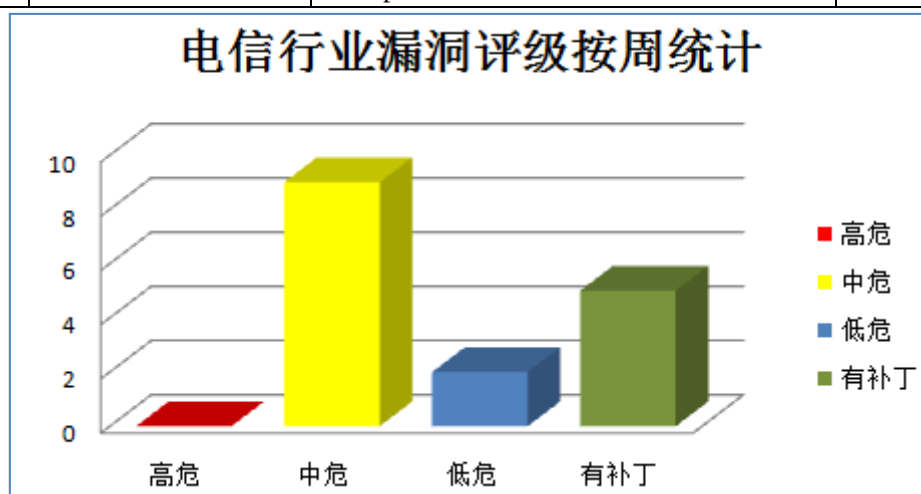


图 1 电信行业漏洞统计

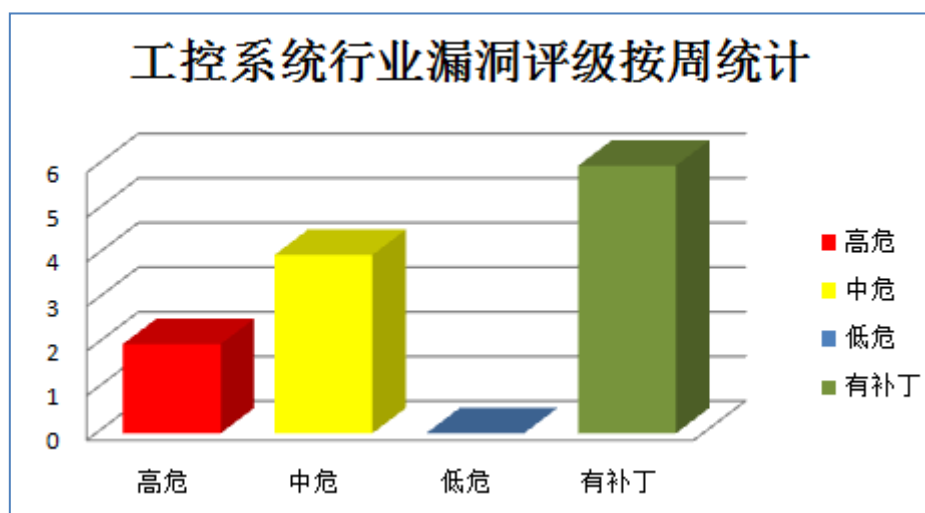


图 2 工控系统行业漏洞统计

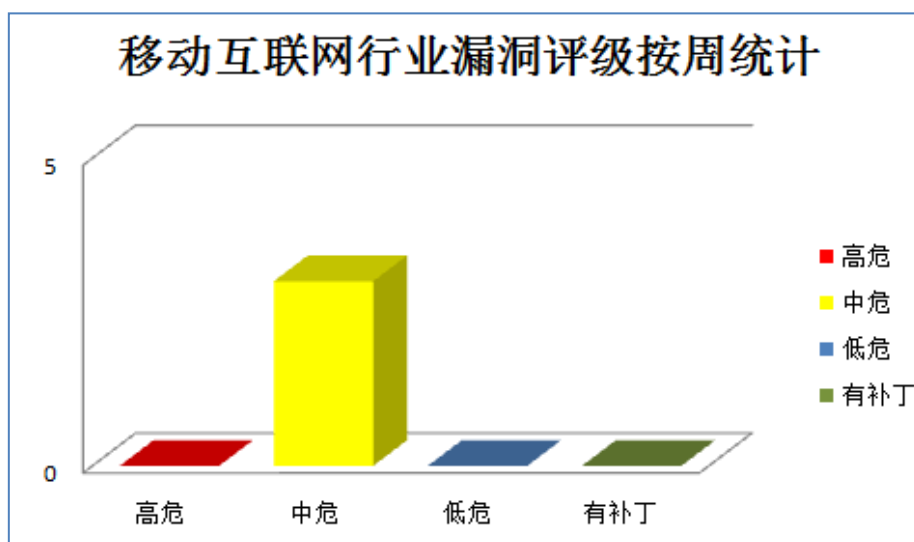


图 3 移动互联网行业漏洞统计

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、Novell 产品安全漏洞

SUSE inst-source-utils 是一套用于创建自定义软件包来源的工具；SUSE Manager for SUSE Linux Enterprise (SLE) 是一套系统管理解决方案；SUSE YaST (Yet another Setup Tool) 是一套以 RPM 为基础的 openSUSE 和 SUSE Linux Enterprise 操作系统的安装与配置工具；USE Zypper 是一款命令行包管理器。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可提升权限，获取敏感信息，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Novell SUSE inst-source-utils 权限提升漏洞、Novell

SUSE Linux Enterprise 竞争条件漏洞、Novell SUSE YaST 信息泄露漏洞、Novell SUSE Linux Enterprise 跨站脚本漏洞、Novell SUSE Zypper 'zypp-refresh-wrapper'任意文件创建漏洞、Novell Open Enterprise Server novell-nrm HTTPSTK 服务链接远程拒绝服务漏洞、Novell iPrint Client 'id1.GetPrinterURLList()'函数远程拒绝服务漏洞。其中，“Novell SUSE inst-source-utils 权限提升漏洞、Novell SUSE Linux Enterprise 竞争条件漏洞、Novell SUSE YaST 信息泄露漏洞”的综合评级为“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-2013-14878>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14876>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14877>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14874>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14875>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14837>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14838>

2、Cybozu 产品安全漏洞

Cybozu Garoon 是一款日文 OA 办公软件系统。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可获取敏感信息或劫持用户会话。

CNVD 收录的相关漏洞包括：Cybozu Garoon 存在未明跨站脚本漏洞（CNVD-2013-14883、CNVD-2013-14884、CNVD-2013-14885、CNVD-2013-14886、CNVD-2013-14887、CNVD-2013-14888、CNVD-2013-14889、CNVD-2013-14890）等。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-2013-14883>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14884>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14885>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14886>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14887>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14888>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14889>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14890>

3、Cisco 产品安全漏洞

Cisco ONS 15454 是一款多业务传输平台；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；Cisco Adaptive Security Appliance 是一款自适应安全设备；Cisco Prime 是一款以服务为中心从终端、网络设备和应用整合管理有线与无线 LAN、WAN 与数据中心，并筛选信息的解决方案；Cisco Secure ACS 是一款 Cisco 网络

设备的中央管理平台。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，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco ONS 15454 控制器卡拒绝服务漏洞（CNVD-2013-14904）、Cisco ONS 15454 控制器卡拒绝服务漏洞、Cisco IOS Software IP Device tracking 拒绝服务漏洞、Cisco IOS XR Software SNMP 请求处理远程拒绝服务漏洞、Cisco IOS XE Software MPLS 报文处理远程拒绝服务漏洞、Cisco ASA Software 畸形 DNS 应答拒绝服务漏洞、Cisco Prime Collaboration Assurance 跨站脚本漏洞、Cisco Secure ACS 非特权 Supoort-Bundle 下载漏洞等。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-2013-14904>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14870>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14871>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14809>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14810>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14843>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14869>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14842>

4、Apache 产品安全漏洞

Apache Solr 是一款开源的搜索服务器。本周，该产品被披露存在多个漏洞，攻击者利用漏洞可发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apache Solr XML 外部实体注入漏洞（CNVD-2013-14818）、Apache Solr XML 外部实体注入漏洞。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-2013-14818>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14819>

5、FlashComs Chat 'file.php'任意文件上传漏洞

FlashComs Chat 是一款基于 Flash 的聊天软件。本周，FlashComs Chat 被披露存在一个综合评级为“高危”的文件上传漏洞，FlashComs Chat 'file.php'未能正确校验上传文件扩展名，远程攻击者利用漏洞提交特殊的文件，并以 WEB 权限执行。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-2013-14866>

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-2013-14880	OSEHRA VistA M2M Broker 验证绕过漏洞	高	请安装厂商已发布的最新版本或补丁： http://www.osehra.org/blog/m2m-broker-security-patch
CNVD-2013-14909	Zabbix Agent Flexible User 参数换行处理远程命令执行漏洞	高	Zabbix Agent 1.8.19rc1, 2.0.10rc1, 2.2.1rc1, 2.3.0 已经修复该漏洞，建议用户下载更新： http://www.zabbix.com/
CNVD-2013-14912	Tftpd32 客户端'Remote File'字段格式串漏洞	高	Tftpd32 Client 4.50 已经修复该漏洞，建议用户下载更新： http://tftpd32.jounin.net/
CNVD-2013-14853	CoolPlayer+ Portable '.m3u'文件缓冲区溢出漏洞	高	暂无
CNVD-2013-14834	Joomla! All Video Share 组件'avsssearch' SQL 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://allvideoshare.mrvinoth.com/
CNVD-2013-14847	Potplayer DLL 加载任意代码执行漏洞	高	Daum PotPlayer 1.5.39659 已经修复该漏洞，建议更新： http://tvpot.daum.net/video/live/PotplayerSpec.d
CNVD-2013-14815	ClientExec 存在多个 SQL 注入漏洞	高	ClientExec 4.6.8 已经修复该漏洞，建议用户下载更新： https://www.clientexec.com/index.php
CNVD-2013-14817	Watermark Master '.wstyle'文件处理远程缓冲区溢出漏洞	高	暂无
CNVD-2013-14822	Winamp 存在多个远程内存破坏漏洞	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://www.winamp.com/
CNVD-2013-14811	BZR Player 'codec_mpeg.dll' dll 加载任意代码执行漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Apache Solr、Cybozu Garoon 和 Novell、Cisco 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，使程序崩溃，导致拒绝服务攻击。此外，FlashComs Chat 聊天软件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。

CNVD 整理和发布以下重要安全修补信息。

1、Microsoft 修补 Enhanced Mitigation Experience Toolkit (EMET) 产品漏洞

Microsoft EMET 是微软为应对漏洞而推出的一款安全工具。本周，Microsoft 修补了 Microsoft EMET 4.0 之前版本存在的安全绕过漏洞，避免攻击者利用漏洞通过 ROP 攻击来绕过 ASLR 保护机制，执行恶意代码。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/41417>



本周要闻速递

1. 支付宝 IOS 端被曝安全漏洞

据苹果网消息，近日，网络上曝出 iOS 端手机支付宝存在解锁漏洞：手机在没有网络的情况下，连续输错五次支付宝图形密码，就可以重新设置图形密码，之后就能直接进入支付宝账户。在该漏洞尚未来修复前，建议尽量不要使用图形密码；此外，最好关闭小额免密支付功能，设置进入支付宝付款时必须输入支付密码。

参考链接：http://finance.ifeng.com/a/20131209/11237321_0.shtml

2. BbocWeb 存上传漏洞

近日，BocWebCMS 系统被披露存在的上传漏洞。黑客可利用该漏洞上传恶意脚本到目标网站根目录下，获取敏感信息，甚至直接控制网站。BocWeb 是国内主流的网站建设系统之一，主要服务于国内企业及行业用户。BocWeb 系统的 uploadify 上传插件由于权限控制不当，导致黑客可以将任意文件上传到目标网站的根目录下。如果向目标网站上传恶意脚本，黑客就能够直接获取到网站敏感数据，甚至直接控制网站，将危害到万科、保利、吉利汽车、珀莱雅、浙江广厦数百家地产、电器、汽车等行业企业的网站。

参考链接：<http://finance.21cn.com/stock/express/a/2013/1205/15/25374373.shtml>

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