

信息安全漏洞周报

2013 年 11 月 11 日-2013 年 11 月 17 日

2013 年第 46 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 164 个，其中高危漏洞 63 个、中危漏洞 87 个、低危漏洞 14 个。上述漏洞中，可利用来实施远程攻击的漏洞有 153 个。本周收录的漏洞中，已有 133 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“PHP RSS Reader URI SQL 注入漏洞”、“Hanso Player '.ogg'文件远程缓冲区溢出漏洞”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 5 家成员单位及个人报送了本周收录的全部 164 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、绿盟科技等单位报送数量较多。此外，个人报送者向 CNVD 提交了 7 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	194	0
启明星辰	114	0
天融信	83	0
绿盟科技	63	0
恒安嘉新	37	0
个人	7	7
报送总计	498	7
录入总计	164（去重）	7

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Microsoft、IBM、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	Microsoft	21	13%
2	IBM	18	11%
3	Cisco	12	7%
4	Google	11	7%
5	Sybase	10	6%
6	Super Micro Computer, Inc	7	4%
7	Drupal	7	4%
8	Adobe	4	2%
9	WordPress	4	2%
10	其它	70	44%

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 164 个漏洞。其中应用程序漏洞 103 个，WEB 应用漏洞 25 个，操作系统漏洞 12 个，网络设备漏洞 11 个，安全产品漏洞 3 个，数据库漏洞 10 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	103
WEB 应用漏洞	25
网络设备漏洞	11
操作系统漏洞	12
安全产品漏洞	3
数据库漏洞	10

表 3 漏洞按影响类型统计表

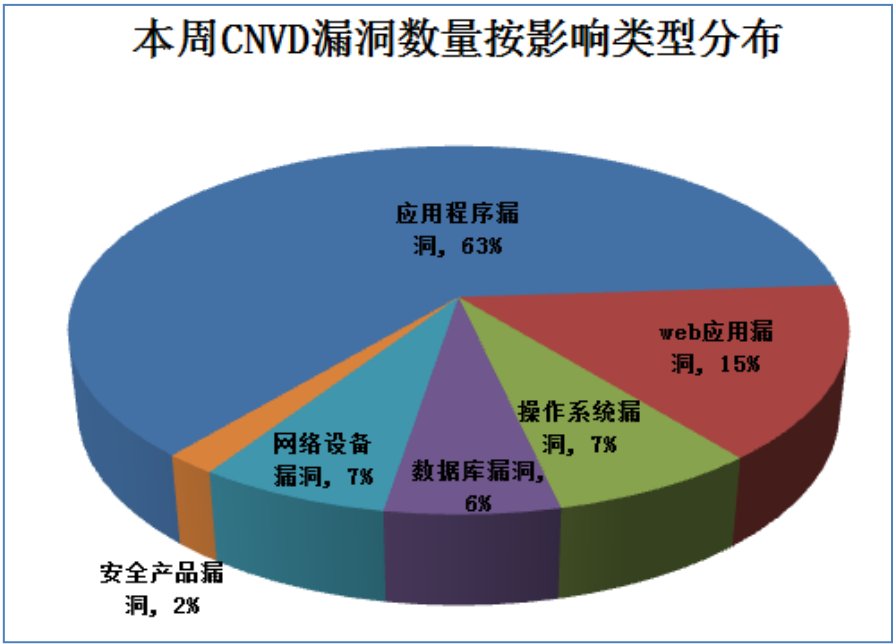


图 1 本周漏洞按影响类型分布



本周行业漏洞信息

本周，CNVD 收录了 21 个电信行业漏洞和 3 个移动互联网行业漏洞（如下列表所示）。其中，“IBM WebSphere Portal URL 操作信息泄露漏洞、Sybase Adaptive Server Enterprise 存在未授权检查漏洞、Sybase Adaptive Server Enterprise 存在未明代码执行漏洞（CNVD-2013-14362）、Sybase Adaptive Server Enterprise 存在未明代码执行漏洞、Sybase Adaptive Server Enterprise 存在未明特权提升漏洞、Cisco IOS SIP 远程拒绝服务漏洞”的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。本周，CNVD 未收录工控系统行业漏洞。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-14474	Cisco NX-OS Software for Nexus 4000 Series 拒绝服务漏洞	中	是
电信	CNVD-2013-14475	Cisco Wireless LAN Controller 存在多个拒绝服务漏洞	中	否
电信	CNVD-2013-14476	Cisco Unified IP Phone 8900/9900 Series 不安全文件权限漏洞	中	是
电信	CNVD-2013-14483	Juniper Networks JUNOS EmbedThis AppWeb web 服务器跨站脚本漏洞	中	是
电信	CNVD-2013-14449	IBM WebSphere Portal URL 操作信息泄露漏洞	高	是

电信	CNVD-2013-14450	IBM WebSphere Portal tagging 跨站脚本漏洞	低	是
电信	CNVD-2013-14451	IBM WebSphere Portal 跨站脚本漏洞	低	是
电信	CNVD-2013-14457	Cisco IOS 内容服务网关安全绕过漏洞	中	是
电信	CNVD-2013-14456	D-Link DSL-2760U-BN 存在多个漏洞	中	否
电信	CNVD-2013-14417	Cisco IOS XR 'OSPFv3'功能拒绝服务漏洞	中	是
电信	CNVD-2013-14359	Sybase Adaptive Server Enterprise 存在未明授权检查漏洞	高	是
电信	CNVD-2013-14360	Sybase Adaptive Server Enterprise 存在未明信息泄露漏洞（CNVD-2013-14360）	中	是
电信	CNVD-2013-14361	Sybase Adaptive Server Enterprise 存在未明拒绝服务漏洞（CNVD-2013-14361）	中	是
电信	CNVD-2013-14362	Sybase Adaptive Server Enterprise 存在未明代码执行漏洞（CNVD-2013-14362）	高	是
电信	CNVD-2013-14354	Sybase Adaptive Server Enterprise 存在未明代码执行漏洞	高	是
电信	CNVD-2013-14355	Sybase Adaptive Server Enterprise 存在未明目录遍历漏洞	中	是
电信	CNVD-2013-14356	Sybase Adaptive Server Enterprise 存在未明特权提升漏洞	高	是
电信	CNVD-2013-14357	Sybase Adaptive Server Enterprise 存在未明拒绝服务漏洞	中	是
电信	CNVD-2013-14358	Sybase Adaptive Server Enterprise 存在未明信息泄漏漏洞（CNVD-2013-14358）	中	是
电信	CNVD-2013-14350	Cisco IOS SIP 远程拒绝服务漏洞	高	是
电信	CNVD-2013-14353	Apache Tomcat 应用跨站请求伪造漏洞	低	否
移动互联网	CNVD-2013-14394	Goodix GT91 触屏驱动 for android 内容长度操作存在多个内存破坏漏洞	中	是

移动互联 网	CNVD-2013-14395	Goodix GT91 触屏驱动 for android 全局变量并发执行输入校验绕过漏洞	中	是
移动互联 网	CNVD-2013-14346	Google Android 签名验证安全绕过漏洞	中	否

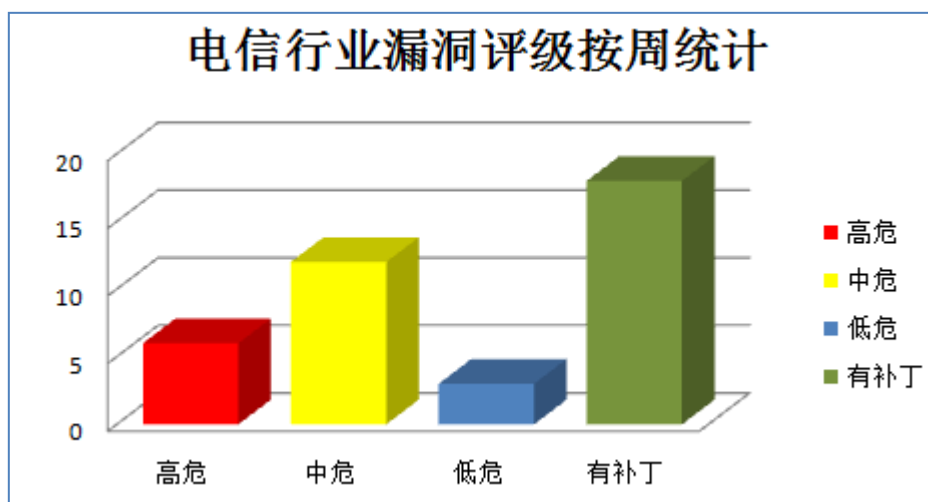


图 1 电信行业漏洞统计

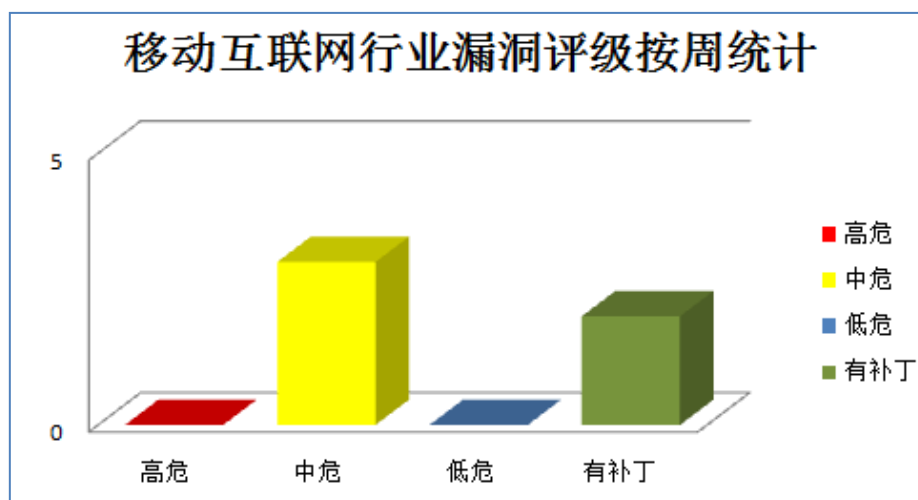


图 2 移动互联网行业漏洞统计

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、Microsoft 产品安全漏洞

11 月 13 日，微软发布了 2013 年 11 月份的月度例行安全公告，共含 8 项更新，修复了 Microsoft Windows、Internet Explorer、Office 中存在的 19 个安全漏洞。其中，

MS13-088、MS13-089、MS13-090 和 MS13-091 项更新综合评级均为最高级“严重”级别，剩余 4 项更新综合评级均为“重要”级别。利用上述漏洞，攻击者可以执行任意代码，提升权限，进行拒绝服务攻击，获取敏感信息。

CNVD 收录的相关漏洞包括：Microsoft Windows 图形设备接口远程代码执行漏洞、Microsoft Office WPD 文件格式内存破坏漏洞、Microsoft Internet Explorer 内存破坏漏洞（CNVD-2013-14464、CNVD-2013-14420、CNVD-2013-14430）、Microsoft Windows Hyper-V 地址破坏权限提升漏洞、Microsoft IE 存在未明越界内存访问任意代码执行漏洞、Microsoft IE ActiveX 控件远程代码执行漏洞等。上述漏洞的综合评级均为“高危”。厂商已经发布了漏洞修补程序。CNVD 提醒广大 Microsoft 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-2013-14460>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14461>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14464>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14465>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14420>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14383>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14434>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14430>

2、Google Chrome 安全漏洞

Google Chrome 是一款 WEB 浏览器。本周，该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，使应用程序崩溃，执行任意命令。

CNVD 收录的相关漏洞包括：Google Chrome 语音输入元素内存错误引用远程代码执行漏洞、Google Chrome media 元素处理内存错误引用远程代码执行漏洞、Google Chrome 'id'属性字符串内存错误引用远程代码执行漏洞、Google Chrome 存在多个未明漏洞、Google Chrome 'libjingle'内存错误引用远程代码执行漏洞、Google Chrome SVG 越界内存破坏漏洞、Google Chrome SVG 越界内存破坏漏洞、Google Chrome 地址栏伪造漏洞（CNVD-2013-14495）等。其中，除“Google Chrome 'libjingle'内存错误引用远程代码执行漏洞、Google Chrome SVG 越界内存破坏漏洞、Google Chrome SVG 越界内存破坏漏洞、Google Chrome 地址栏伪造漏洞（CNVD-2013-14495）”外，其余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-2013-14500>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14499>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14497>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14485>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14484>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14498>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14346>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14495>

3、Adobe 产品安全漏洞

Adobe Flash Player 是一款 Flash 文件处理程序；Adobe Air 是一款 Adobe 公司出品的跨操作系统的运行时库；Adobe ColdFusion 是一个动态 Web 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，使应用程序崩溃，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player / AIR 存在未明内存破坏漏洞（CNVD-2013-14489、CNVD-2013-14490）、Adobe ColdFusion 存在未明远程读访问漏洞、Adobe ColdFusion CFIDE 目录存在未明反射型跨站脚本漏洞。其中，除“Adobe ColdFusion CFIDE 目录存在未明反射型跨站脚本漏洞”外，其余漏洞的综合评级为“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-2013-14489>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14490>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14492>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14491>

4、Cisco 产品安全漏洞

Cisco IOS 是多数思科系统路由器和网络交换机上使用的互连网络操作系统；Cisco TelePresence VX- Clinical Assistant 是一款供医疗环境中使用的专用移动远程医疗工具推车；Cisco WAAS Mobile server 是一款针对移动用户应用加速的解决方案；Cisco Adaptive Security Appliance 是一款自适应安全设备，可提供安全和 VPN 服务的模块；Cisco Nexus 系列交换机是数据中心级交换机，采用 Cisco Nexus OS 操作系统。本周，上述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，执行任意代码。

CNVD 收录的相关漏洞包括：Cisco IOS SIP 远程拒绝服务漏洞、Cisco TelePresence VX Clinical Assistant 管理密码重置漏洞、Cisco WAAS Mobile WEB 接口远程代码执行漏洞、Cisco Adaptive Security Appliance (ASA)特制自动升级数据处理远程拒绝服务漏洞、Cisco Adaptive Security Appliance (ASA)电话代理数据库项操作漏洞、Cisco IOS 内容服务网关安全绕过漏洞、Cisco NX-OS Software for Nexus 4000 Series 拒绝服务漏洞。其中，“Cisco IOS SIP 远程拒绝服务漏洞、Cisco TelePresence VX Clinical Assistant 管理密码重置漏洞、Cisco WAAS Mobile WEB 接口远程代码执行漏洞”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-2013-14350>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14349>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14348>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14398>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14397>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14457>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-14474>

5、PHP RSS Reader URI SQL 注入漏洞

PHP RSS Reader 实现 RSS 阅读器功能，负责数据库文件和程序部署说明文档。本周，PHP RSS Reader 被披露存在一个综合评级为“高危”的 SQL 注入漏洞。由于程序未能正确过滤通过 URL 提交的用户输入，远程攻击者利用漏洞可进行 SQL 注入攻击，操作或获取数据库信息，或获得 WEB SHELL。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-2013-14447>

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-2013-14481	libjpeg-turbo 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： https://code.google.com/p/chromium/issues/detail?id=299835
CNVD-2013-14487	ClubDJ ProVJ '.m3u'远程缓冲区溢出漏洞	高	暂无
CNVD-2013-14449	IBM WebSphere Portal URL 操作信息泄露漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： http://www-01.ibm.com/support/docview.wss?uid=swg21655656
CNVD-2013-14437	Supermicro IPMI 'close_window.cgi' 调用多个参数缓冲区溢出漏洞	高	暂无
CNVD-2013-14455	gitlab-shell 知识库导入功能远程代码执行漏洞	高	Gitlab 已经修复该漏洞，建议用户下载更新： https://gitlab.com/gitlab-org/gitlab-shell https://gitlab.com/gitlab-org

CNVD-2013-14446	RASPcalendar 管理登录页存在多个 SQL 注入漏洞	高	暂无
CNVD-2013-14403	SaltStack Salt 'salt/utils/verify.py' 权限提升漏洞	高	Salt (aka SaltStack) 0.17.1 已经修复该漏洞，建议用户下载更新： http://www.saltstack.com/topics/releases/0.17.1.html
CNVD-2013-14447	PHP RSS Reader URI SQL 注入漏洞	高	暂无
CNVD-2013-14406	metinfo 存在未明 SQL 注入漏洞	高	暂无
CNVD-2013-14431	Webers CMS 存在多个输入验证漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，微软发布了 2013 年 11 月份的月度例行安全公告，共含 8 项更新，修复了 Microsoft Windows、Internet Explorer、Office 中存在的 19 个安全漏洞。利用上述漏洞，攻击者可以执行任意代码，提升权限，进行拒绝服务攻击，获取敏感信息。本周，Google Chrome 和 Adobe、Cisco 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，使应用程序崩溃，执行任意代码。此外，PHP RSS Reader 程序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、libjpeg-turbo 修补 2 个漏洞

libjpeg-turbo 是一个专门为 x86 和 x86-64 处理器优化的高速 libjpeg 的改进版本。libjpeg-turbo 修补两个信息泄露漏洞，避免攻击者利用漏洞构建恶意文件，诱使引用程序解析，读取未初始化内存，获取敏感信息。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/41124>

<http://www.cnvd.org.cn/patchInfo/show/41123>

本周要闻速递

1. 安卓手机 ROOT 普遍存漏洞

国外网站曝出安卓手机 ROOT 必装的权限管理器普遍存在“超级用户”漏洞（SU

漏洞), 国内手机杀毒软件团队第一时间验证该漏洞危害巨大, 手机木马可利用漏洞变身系统超级用户, 从而完全控制手机, 偷话费、窃取短信、通讯录等隐私甚至监听通话, 几乎全部安卓 ROOT 手机均受影响。目前, 360 手机卫士已发布了修复方案, 建议 ROOT 过的安卓手机用户更新到最新版进行体检和漏洞修复。用户也可手动下载安装已修复漏洞的 SuperSU (超级授权) 来管理 ROOT 权限, 避免被手机木马侵害。

参考链接: <http://news.163.com/13/1117/07/9DS96Q1R00014Q4P.html>

2. 两大浏览器漏洞

两大浏览器中以前未被发现的漏洞在 Windows 8.1 和安卓移动设备上暴露出来, 通过 Windows8.1 的 IE 11 和安卓上运行的谷歌 Chrome, 安全研究人员入侵了微软 Surface Pro, Nexus 4 和三星 Galaxy S4 设备。

参考链接: http://security.zdnet.com.cn/security_zone/2013/1118/2995880.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