

信息安全漏洞周报

2013 年 08 月 19 日-2013 年 08 月 25 日

2013 年 第34 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 150 个，其中高危漏洞 50 个、中危漏洞 81 个、低危漏洞 19 个。上述漏洞中，可利用来实施远程攻击的漏洞有 131 个。本周收录的漏洞中，已有 110 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“phpVID 存在多个 SQL 注入漏洞”、“Sounder Gem for Ruby 文件名处理任意命令执行漏洞”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 4 家成员单位及个人报送了本周收录的全部 150 个漏洞。各单位报送情况如表 1 所示。其中，天融信、恒安嘉新、安天实验室、等单位报送数量较多。此外，High-Tech Bridge 和个人报送者向 CNVD 提交了 21 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
天融信	83	0
恒安嘉新	78	0
安天实验室	72	0
绿盟科技	41	0
High-Tech Bridge	3	3
个人	18	18
报送总计	295	21
录入总计	150（去重）	21

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、Microsoft、Puppet Labs、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	IBM	12	8%
2	Microsoft	10	7%
3	Puppet Labs	10	7%
4	Google	9	6%
5	wordpress	4	3%
6	Drupal	4	3%
7	Red Hat	3	2%
8	Linux	3	2%
9	Oracle	2	1%
10	Cisco	1	1%
11	其它	92	60%

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 150 个漏洞。其中应用程序漏洞 101 个，WEB 应用漏洞 35 个，操作系统漏洞 9 个，安全产品漏洞 4 个，网络设备漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	101
WEB 应用漏洞	35
网络设备漏洞	1
操作系统漏洞	9
安全产品漏洞	4
数据库漏洞	0

表 3 漏洞按影响类型统计表

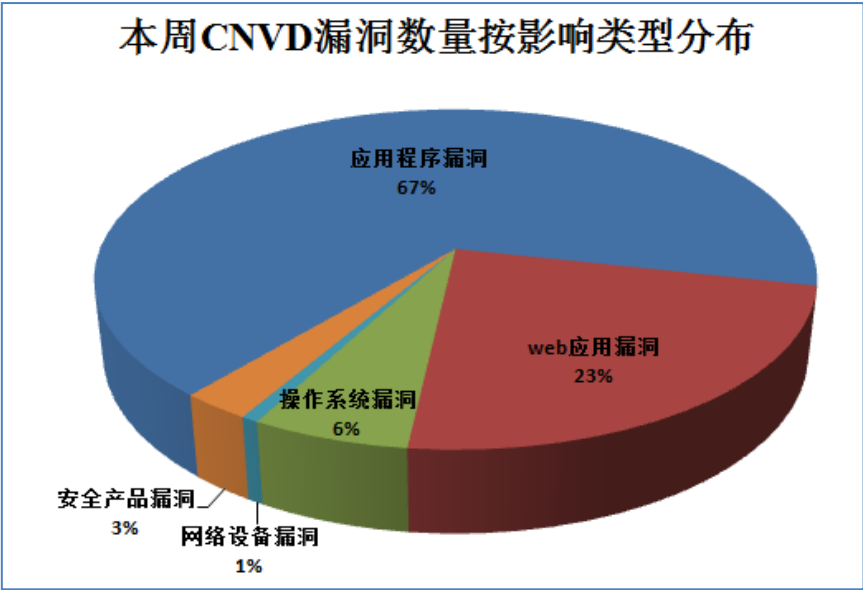


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 9 个电信行业漏洞、3 个移动互联网行业漏洞和 1 个工控系统漏洞（如下列表所示）。其中，“ISC BIND 9 SRTT 算法授权服务器选择安全漏洞、ThinkSNS 存在未明 SQL 注入漏洞、HTC Sync Manager 多个 DLL 加载任意代码执行漏洞、Sixnet Universal Protocol Undocumented 函数代码远程安全绕过漏洞”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-2013-12525	IBM WebSphere Portal 未授权访问漏洞	中危	有补丁
电信	CNVD-2013-12527	IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2013-12527）	低危	有补丁
电信	CNVD-2013-12529	IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2013-12529）	中危	有补丁
电信	CNVD-2013-12531	IBM WebSphere Application Server 跨站请求伪造漏洞（CNVD-2013-12531）	中危	有补丁
电信	CNVD-2013-12530	IBM WebSphere Application Server 信息泄露漏洞（CNVD-2013-12530）	低危	有补丁
电信	CNVD-2013-12532	IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2013-12532）	低危	有补丁
电信	CNVD-2013-12533	IBM WebSphere Application Server 跨站脚本漏洞（CNVD-2013-12533）	低危	有补丁
电信	CNVD-2013-12416	ISC BIND 9 SRTT 算法授权服务器选择安全漏洞	高危	无补丁
电信	CNVD-2013-12421	Cisco IOS XR Software 本地拒绝服务漏洞	中危	有补丁
移动互	CNVD-2013-12547	ThinkSNS 存在未明 SQL 注入漏洞	高危	无补丁

联网				
移动互 联网	CNVD-2013-12506	HTC Sync Manager 多个 DLL 加载任意代码执行 漏洞	高危	无补丁
移动互 联网	CNVD-2013-12509	ACal 'view'参数本地文件包含漏洞	中危	无补丁
工控系 统	CNVD-2013-12528	Sixnet Universal Protocol Undocumented 函数代码 远程安全绕过漏洞	高危	有补丁

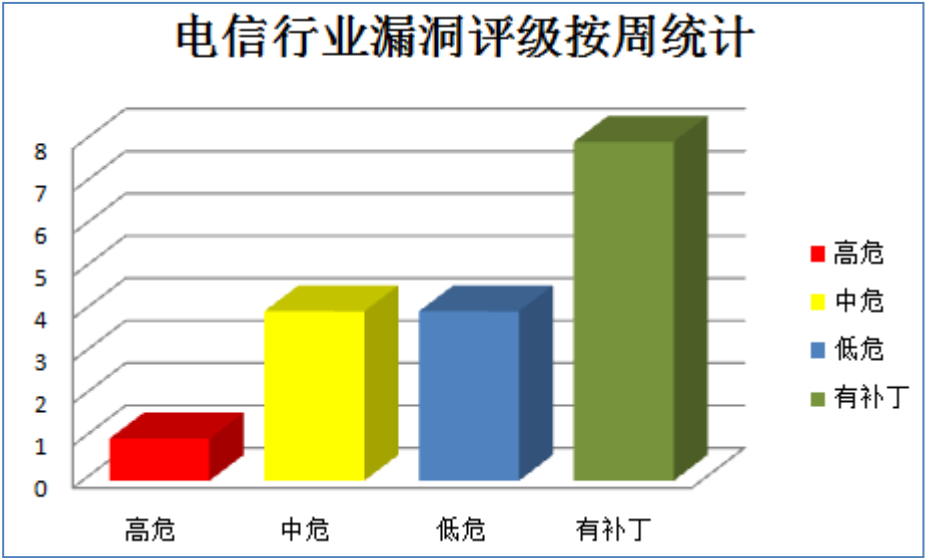


图 2 电信行业漏洞统计

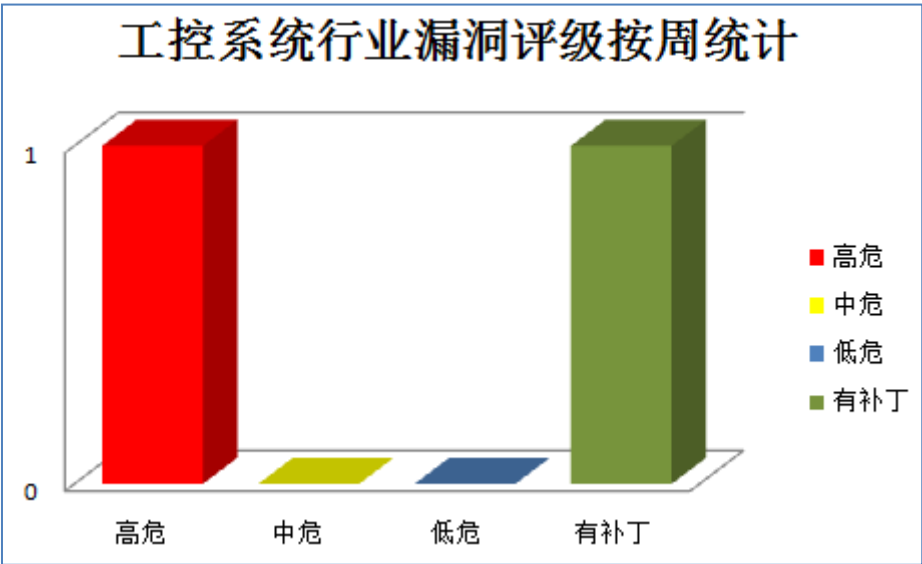


图 3 工控系统行业漏洞统计

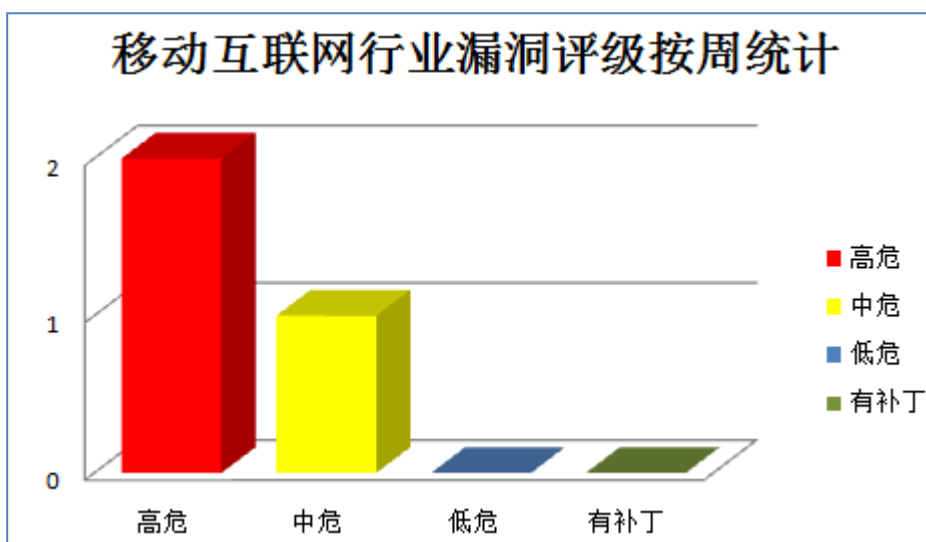


图 4 移动互联网行业漏洞统计

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、Google Chrome 安全漏洞

Google Chrome 是一款 WEB 浏览器。本周，该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，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Chrome 存在多个整数溢出漏洞、Google Chrome 'files/file_path.cc'存在未能漏洞、Google Chrome 'files/file_path.cc'存在未能漏洞、Google Chrome 'XSLT ProcessingInstruction implementation'内存错误引用漏洞、Google Chrome 'core/html/HTMLMediaElement.cpp'内存错误引用漏洞、Google Chrome 存在多个未明漏洞（CNVD-2013-12491）、Google Chrome 信息泄露漏洞（CNVD-2013-12485）、Google Chrome SliderThumbElement::setPositionFromPoint 函数存在未明漏洞等。上述漏洞中除“Google Chrome 信息泄露漏洞（CNVD-2013-12485）、Google Chrome SliderThumbElement::setPositionFromPoint 函数存在未明漏洞”外，其余漏洞的综合评级均为“高危”。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-2013-12486>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12487>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12488>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12489>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12490>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12491>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12485>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12452>

2、IBM 产品安全漏洞

IBM 1754 GCM 系列在单一设备中提供了经由 IP 的 KVM 和串行控制台管理技术；IBM InfoSphere Information Server 是一款数据集成软件平台；WebSphere 是 IBM 的集成软件平台；IBM WebSphere Portal 提供了一个组合应用程序或业务 mashup 框架，并且提供了一种基于 SOA 的解决方案。IBM BladeCenter 是一款高性能企业级服务器。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，执行未授权的访问或执行任意命令。

CNVD 收录的相关漏洞包括：IBM 1754 GCM16 及 GCM32 Global Console Managers 存在多个命令执行漏洞、IBM InfoSphere Information Server 用户枚举漏洞、IBM WebSphere Application Server 跨站请求伪造漏洞(CNVD-2013-12531、CNVD-2013-12529、CNVD-2013-12533)、IBM WebSphere Portal 未授权访问漏洞、IBM BladeCenter 高级管理模块 adv_sw.php 跨站脚本漏洞、IBM BladeCenter 高级管理模块 adv_sw.php 跨站脚本漏洞等。其中，“IBM 1754 GCM16 及 GCM32 Global Console Managers 存在多个命令执行漏洞”的综合评级为“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-2013-12510>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12514>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12531>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12529>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12525>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12508>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12507>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12533>

3、Puppet 安全漏洞

Puppet 是帮助系统管理员管理基础架构的 IT 自动化软件。本周，该产品被披露存在多个安全漏洞。远程攻击者利用漏洞可绕过安全限制，获取敏感信息。

CNVD 收录的相关漏洞包括：Puppet Enterprise 会话劫持漏洞(CNVD-2013-12534)、Puppet Enterprise 会话处理本地安全绕过漏洞、Puppet Enterprise 存在多个信息泄露漏洞、Puppet Enterprise 信息泄露漏洞、Puppet Enterprise 安全绕过漏洞、Puppet Enterprise 会话拦截漏洞、Puppet Enterprise 密码泄露漏洞、Puppet Enterprise 输入验证漏洞等。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-2013-12534>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12535>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12536>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12537>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12538>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12539>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12540>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12495>

4、Drupal 模块安全漏洞

Drupal 是一款使用 PHP 语言开发的内容管理系统。本周，该产品的多个模块被披露存在多个漏洞，攻击者利用漏洞可绕过安全限制，获得敏感信息或执行未授权的操作。

CNVD收录的相关漏洞包括：Drupal RESTful Web Services模块存在多个访问安全绕过漏洞、Drupal Entity API模块存在多个访问绕过漏洞、Drupal BOTCHA模块信息泄露漏洞、Drupal Password Policy模块存在多个跨站脚本漏洞。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-2013-12500>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12460>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12462>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-12463>

5、phpVID 存在多个 SQL 注入漏洞

phpVID 是一款视频分享应用。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。phpVID 包含的 browse_videos.php, groups.php 和 members.php 脚本未能正确过滤用户提交给'n', 'cat', 'n'参数的数据，攻击者利用漏洞可进行 SQL 注入攻击，获取数据库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-2013-12447>

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-2013-12528	Sixnet Universal Protocol Undocumented 函数代码远程安全绕过漏洞	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://ics-cert.us-cert.gov/advisories/ICS-13-231-01
CNVD-2013-12547	ThinkSNS 存在未明 SQL 注入漏洞	高	暂无
CNVD-2013-12542	TYPO3 Store Locator Extension 存在未明 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://typo3.org/teams/security/security-bulletins/typo3-extensions/typo3-ext-sa-2013-013
CNVD-2013-12548	Sounder Gem for Ruby 文件名处理任意命令执行漏洞	高	暂无
CNVD-2013-12543	Graphite 'pickle.loads()'任意代码执行漏洞	高	Graphite 0.9.11 版本已修复此漏洞，建议用户下载使用： http://ceriksen.com/2013/08/20/graphite-remote-code-execution-vulnerability-advisory/
CNVD-2013-12506	HTC Sync Manager 多个 DLL 加载任意代码执行漏洞	高	暂无
CNVD-2013-12550	Oracle Java IntegerInterleavedRaster.verify() 函数整数溢出漏洞	高	Oracle Java JRE 7 Update 25 已经修复此漏洞，建议用户下载更新： http://oracle.com/java
CNVD-2013-12520	FluidGalleries 'photo-upload.php' 任意文件上传漏洞	高	暂无
CNVD-2013-12552	Kepware Technologies DNP Master Driver 拒绝服务漏洞	高	厂商已经修复此漏洞，建议用户下载更新： https://my.kepware.com/mykepware/Login.aspx
CNVD-2013-12469	Quark Chat SQL 注入漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Google Chrome 和 IBM 多款产品被披露存在多个漏洞，远程攻击者利用漏洞可获得敏感信息，执行未授权的访问，发起拒绝服务攻击。Puppet 以及 Drupal 的多个模块被披露存在多个漏洞，攻击者利用漏洞可绕过安全限制获取敏感信息。此外，phpVID 视频分享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、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，攻击者可以利用漏洞破坏内存，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/38281>
<http://www.cnvd.org.cn/patchInfo/show/38251>
<http://www.cnvd.org.cn/patchInfo/show/38250>



本周要闻速递

1. Facebook 现漏洞

据美国科技博客 TheVerge 报道, 安全研究员卡利勒·史莱特(Khalil Shreatch)近日发现 Facebook(40.55, 2.00, 5.19%)存在重大漏洞, 并利用该漏洞在 Facebook CEO 马克·扎克伯格(Mark Zuckerberg)的页面上留言。史莱特虽未因发现该漏洞而获得奖励, 但其支持者已通过众筹方式共筹得 11000 美元。

参考链接: <http://tech.sina.com.cn/i/2013-08-22/07528663498.shtml>

2. Nexus 7 更新软件修复触摸屏失灵漏洞

不久前谷歌 Nexus 7 二代曝出了 GPS 系统问题, 在导航的途中会莫名其妙的自己中断, 谷歌目前仍在努力修复中, 尚未给出最终的修复方案。这个问题还没有被解决, Nexus 7 二代又曝出新的问题: 触摸屏失灵。在点击 Nexus 7 二代的时候屏幕会失灵, 而且现在这个状况不是个例。这次谷歌反应的够快, 已经放出针对 Nexus 7 二代的软件升级, 修复了这一漏洞。这次漏洞的更新版本为 JSS15Q, 如今购买过 Nexus 7 二代的消费者都将会收到这次更新的实时推送, 但由于购买国家人民所处的时区不同, 因此在更新时间上不是特别统一, 即便如此收到漏洞修复的推送还是一个不错的消息, 我们也希望谷歌能够再接再厉把这款平板的不稳定因素降到最低。

参考链接: <http://pad.cnmo.com/28/282739.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