

## 信息安全漏洞周报

2012 年 8 月 6 日-2012 年 8 月 12 日

2012 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 103 个，其中高危漏洞 21 个、中危漏洞 76 个、低危漏洞 6 个。上述漏洞中，可利用来实施远程攻击的漏洞有 89 个。本周收录的漏洞中，已有 74 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“OTRS 'Body' HTML 注入漏洞”、“ligra Calligra 堆缓冲区溢出漏洞（CNVD-2012-13487）”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 7 家成员单位和多个合作伙伴及个人报送了本周收录的全部 103 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、天融信、绿盟科技、安天实验室等单位报送数量较多。此外，天融信、网御星云、广西网信、上海交通大学以及个人报送者向 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 |
|---------|--------|--------|
| 启明星辰    | 73     | 0      |
| 天融信     | 69     | 1      |
| 绿盟科技    | 62     | 0      |
| 安天实验室   | 33     | 0      |
| 恒安嘉新    | 18     | 0      |
| 安氏领信    | 10     | 0      |
| 东软      | 3      | 0      |
| 网御星云    | 1      | 1      |
| 广西网信    | 1      | 1      |

|        |         |   |
|--------|---------|---|
| 上海交通大学 | 1       | 1 |
| 个人     | 3       | 3 |
| 报送总计   | 274     | 7 |
| 录入总计   | 103（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 Cisco、Debian、IBM、Oracle 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  | Cisco     | 20   | 19%  |
| 2  | Debian    | 5    | 5%   |
| 3  | IBM       | 3    | 3%   |
| 4  | Oracle    | 3    | 3%   |
| 5  | TYPO3     | 3    | 3%   |
| 6  | PBBoard   | 3    | 3%   |
| 7  | Wordpress | 3    | 3%   |
| 8  | HP        | 2    | 2%   |
| 9  | JBoss     | 2    | 2%   |
| 10 | Google    | 2    | 2%   |
| 11 | 其它        | 57   | 55%  |

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 108 个漏洞。其中操作系统漏洞 10 个，应用程序漏洞 49 个，WEB 应用漏洞 26 个，数据库漏洞 1 个，网络设备漏洞 12 个，安全产品漏洞 5 个。

| 漏洞影响对象类型 | 漏洞数量 |
|----------|------|
| 操作系统漏洞   | 10   |
| 应用程序漏洞   | 49   |
| WEB 应用漏洞 | 26   |
| 网络设备漏洞   | 12   |
| 数据库漏洞    | 1    |
| 安全产品漏洞   | 5    |

表 3 漏洞按影响类型统计表

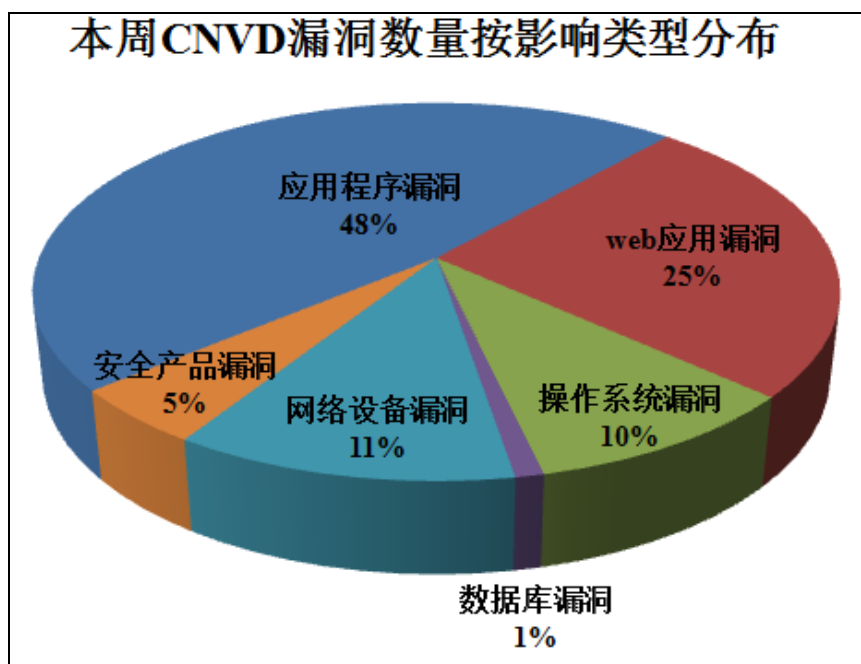


图 1 本周漏洞按影响类型分布

## 本周涉及电信行业漏洞信息

本周，CNVD 收录了 12 个网络设备漏洞：“Aironet access points 远程拒绝服务漏洞、Cisco Catalyst 3560 和 3750 拒绝服务漏洞、Cisco Carrier Routing System ACL 绕过漏洞、Cisco Emergency Responder UDP 报文拒绝服务漏洞、Cisco IOS clientless SSL VPN 拒绝服务漏洞、Cisco IOS 信息泄露漏洞、Cisco MDS 9000 拒绝服务漏洞、Cisco Nexus 设备远程拒绝服务漏洞、Cisco NX-OS CDP 报文拒绝服务漏洞、Cisco IOS SSH2 会话远程拒绝服务漏洞（CNVD-2012-13485）、Citrix Access Gateway 存在多个漏洞、Iomega 网络存储设备安全绕过漏洞”。其中“Iomega 网络存储设备安全绕过漏洞”的综合评级为“高危”。

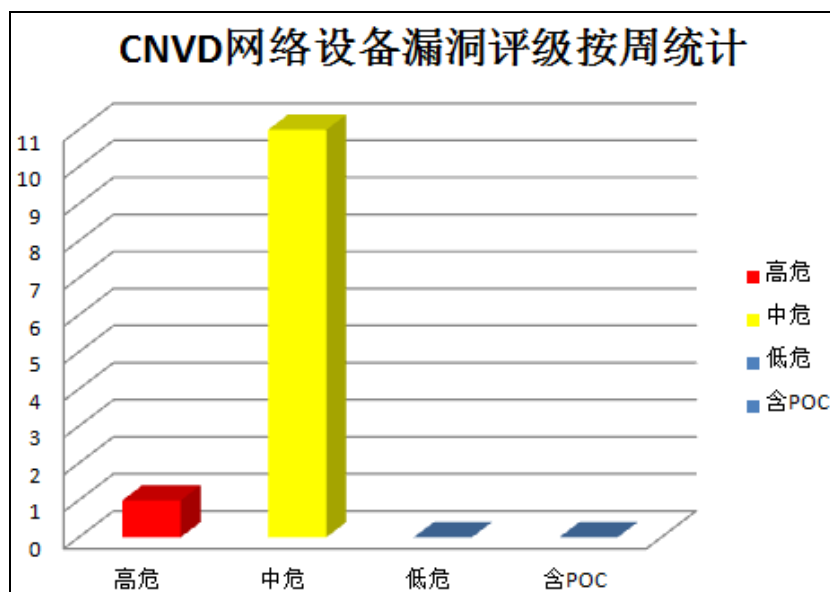


图 2 网络设备漏洞统计

## 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、Cisco 产品安全漏洞

Cisco IOS 是一款思科网络设备操作系统；Cisco IP Communicator 是一款基于 Windows 平台的电话支持应用软件；Cisco Nexus 系列交换机是数据中心级交换机；Cisco AnyConnect Secure Mobility 是一款企业移动安全解决方案；Cisco Carrier Routing System 是一款运营商级路由系统。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取敏感信息，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IOS clientless SSL VPN 拒绝服务漏洞、Cisco IOS 信息泄露漏洞、Cisco IOS SSH2 会话远程拒绝服务漏洞（CNVD-2012-13485）、Cisco IP Communicator 证书修改漏洞、Cisco NX-OS CDP 报文拒绝服务漏洞、Cisco Nexus 设备远程拒绝服务漏洞、Cisco AnyConnect Secure Mobility Client 证书验证安全绕过漏洞（CNVD-2012-13461）、Cisco Carrier Routing System ACL 绕过漏洞等。厂商已经修复了上述漏洞，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/sites/main/preview/ldgg\\_preview.htm?tid=53055](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53055)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=53057](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53057)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=53100](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53100)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=53058](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53058)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=53061](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53061)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=53060](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53060)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=53048](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53048)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=53051](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53051)

## 2、IBM 产品安全漏洞

IBM Rational Directory Server 是为兼容 Rational 工具提供基础架构服务或用户验证、用户管理、组定义、用户数据存储和应用数据存储的解决方案；IBM WebSphere Application Server (WAS)是由 IBM 遵照开放标准，例如 Java EE、XML 、Web Services 等开发的一种应用服务产品；IBM Hardware Management Console 主要提供标准用户接口进行配置和管理 Power System 系列服务器。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获得敏感信息或劫持用户会话，以 root 权限执行任意命令。

CNVD 收录的相关漏洞包括：IBM 多个产品本地特权提升漏洞（CNVD-2012-13495）、IBM WebSphere Application Server 存在未明跨站脚本漏洞、IBM Rational Directory Server 存在多个漏洞。其中，“IBM 多个产品本地特权提升漏洞（CNVD-2012-13495）”的综合评级为“高危”。目前，厂商已经修复了上述漏洞。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/sites/main/preview/ldgg\\_preview.htm?tid=53159](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53159)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=53158](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53158)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=53039](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53039)

## 3、Sielco Sistemi Winlog 安全漏洞

SIELCO SISTEMI Winlog 是一款 SCADA HMI 数据采集和远程控制的工业控制系统软件。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系统崩溃，发起拒绝服务攻击或执行任意代码。

CNVD 收录的相关漏洞包括：Sielco Sistemi Winlog 应用存在漏洞（CNVD-2012-13435、CNVD-2012-13434、CNVD-2012-13433、CNVD-2012-13432）。上述漏洞的综合评级均为“高危”，厂商已经修复了上述漏洞。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/sites/main/preview/ldgg\\_preview.htm?tid=52972](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52972)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=52971](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52971)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=52970](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52970)

[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=52969](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=52969)

## 4、Oracle 产品安全漏洞

Oracle Business Transaction Management (BTM)是一款对分布式、模块化的组合应用程序中的业务事务进行端到端管理的软件；Oracle Sun Solaris 是一款商用操作系统。本周，上述产品被披露存在多个漏洞，攻击者利用漏洞可以以管理员权限通过目录遍历攻击，删除系统文件，向目标服务器写任意文件。

CNVD 收录的相关漏洞包括：Oracle Sun Products Suite Solaris mailx 本地漏洞、Oracle Business Transaction Management Server 任意文件写/删除漏洞。其中，“Oracle

Business Transaction Management Server 任意文件写/删除漏洞”的综合评级均为“高危”，厂商已经修复了“Oracle Sun Products Suite Solaris mailx 本地漏洞”。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/sites/main/preview/ldgg\\_preview.htm?tid=53164](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53164)  
[http://www.cnvd.org.cn/sites/main/preview/ldgg\\_preview.htm?tid=53098](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53098)

## 5、OTRS 'Body' HTML 注入漏洞

OTRS Open Technology Real Service 是一款开源的桌面和 IT 服务管理解决方案。本周，OTRS Open Technology Real Service 被披露存在一个 SQL 注入漏洞。由于 OTRS 未能对'Body'字段进行充分过滤，攻击者可以利用漏洞进行存储型跨站脚本攻击，可获得敏感信息或劫持用户会话。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/sites/main/preview/ldgg\\_preview.htm?tid=53210](http://www.cnvd.org.cn/sites/main/preview/ldgg_preview.htm?tid=53210)

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/publish/main/52/index.html>

| CNVD 编号         | 漏洞名称                                           | 综合评级 | 修复方式                                                                                                                                                                                                        |
|-----------------|------------------------------------------------|------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CNVD-2012-13503 | Ubisoft Uplay ActiveX 控件任意代码执行漏洞               | 高    | 暂无                                                                                                                                                                                                          |
| CNVD-2012-13489 | Bitcoin-Qt 拒绝服务漏洞                              | 高    | 用户可参考如下供应商提供的安全公告获得补丁信息：<br><a href="https://github.com/bitcoin/bitcoin/commit/8864019f6d88b13d3442843d9e6eb8dd938831">https://github.com/bitcoin/bitcoin/commit/8864019f6d88b13d3442843d9e6eb8dd938831</a> |
| CNVD-2012-13480 | NVIDIA Linux Driver VGA Window 本地权限提升漏洞        | 高    | 暂无                                                                                                                                                                                                          |
| CNVD-2012-13430 | Siemens Synco OZW 不安全默认密码漏洞                    | 高    | 西门子已经为 OZW672 和 OZW772 设备发布了升级固件，用户可联系供应商获得相应的补丁程序：<br><a href="http://subscriber.communications.siemens.com/">http://subscriber.communications.siemens.com/</a>                                            |
| CNVD-2012-13492 | Dir2web SQL 注入漏洞                               | 高    | 暂无                                                                                                                                                                                                          |
| CNVD-2012-13482 | Ubisoft Entertainment UPLAY 'OBJECT'控件远程命令执行漏洞 | 高    | 暂无                                                                                                                                                                                                          |
| CNVD-2012-13422 | LibreOffice 和 OpenOffice 基于堆的缓冲区溢出漏洞           | 高    | LibreOffice 3.5.5 或 3.6.0 已经修复此漏洞，建议用户下载使用：                                                                                                                                                                 |

|                 |                                          |   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------|------------------------------------------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                 |                                          |   | <a href="http://www.libreoffice.org">http://www.libreoffice.org</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| CNVD-2012-13501 | Joomla! En Masse 组件'sortBy' SQL 注入漏洞     | 高 | 暂无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| CNVD-2012-13429 | Opera Web Browser 远程代码执行漏洞               | 高 | Opera Web Browser 12.01 或 11.66 (Mac OS X 平台)已经修复此漏洞，建议用户下载使用：<br><a href="http://www.opera.com/">http://www.opera.com/</a>                                                                                                                                                                                                                                                                                                                                                                                                   |
| CNVD-2012-13451 | AOL downloadUpdater2 插件 'SRC'参数远程缓冲区溢出漏洞 |   | 暂无                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| CNVD-2012-13499 | OpenStack Nova 内存破坏漏洞                    | 高 | 用户可参考如下供应商提供的安全公告获得补丁信息： Folsom fix: <a href="https://github.com/openstack/nova/commit/ce4b2e27be45a85b310237615c47eb53f37bb5f3">https://github.com/openstack/nova/commit/ce4b2e27be45a85b310237615c47eb53f37bb5f3</a> Essex fix: <a href="https://github.com/openstack/nova/commit/d9577ce9f266166a297488445b5b0c93c1ddb368">https://github.com/openstack/nova/commit/d9577ce9f266166a297488445b5b0c93c1ddb368</a> Diablo fix: <a href="https://review.openstack.org/#/c/10953/">https://review.openstack.org/#/c/10953/</a> |

表 3 部分高危漏洞列表

小结：本周，Cisco 以及 IBM 的多个产品被披露存在多个漏洞，攻击者利用漏洞可获取敏感信息或发起拒绝服务攻击。SIELCO SISTEMI 以及 Siemens 等公司的工业控制系统产品存在的漏洞可被利用发起拒绝服务攻击或执行任意代码。Oracle 的两款产品被披露存在漏洞，攻击者利用漏洞可以以管理员权限，取得主机操作系统的执行权限。此外，OTRS Open Technology Real Service 被披露存在零日漏洞，对网络服务器安全构成威胁，相关用户需加强防范。

## 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、Google 发布升级程序，修补 Chrome 安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，Google 发布升级程序，修补了 Chrome 存在的漏洞。允许攻击者构建恶意 WEB 页，诱使用户解析，可以应用程序上下文执行任意代码。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/sites/main/preview/bdgg\\_preview.htm?tid=19642](http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=19642)  
[http://www.cnvd.org.cn/sites/main/preview/bdgg\\_preview.htm?tid=19640](http://www.cnvd.org.cn/sites/main/preview/bdgg_preview.htm?tid=19640)



## 本周要闻速递

### 1. 苹果中止电话重置密码修补 iCloud 漏洞

8月9日消息，据国外媒体报道，苹果目前已经暂时修补了 iCloud 账户安全漏洞。此漏洞曾导致用户的账户被黑客暴力破解。苹果已经给我们就重设苹果账户密码这一事件给出了官方的说法。苹果确认了他们已经暂时中止了通过电话重设密码的这种操作，并且鼓励用户通过网络更改密码。这个系统可以通过两种方式重置密码，一种是把重设密码的请求发送至另一个已经注册的邮箱里，或者通过正确回答用户之前已经设置好的安全提问来完成。当恢复电话修改密码时，用户将要通过一个更强的身份验证机制来重新设置他们的密码。

参考链接：<http://tech.163.com/12/0809/02/88EBQLHG000915BD.html>

### 2. Android 平台 Yahoo 程序漏洞被滥用

就在一波疑似某 Android 僵尸网络垃圾邮件的报导出现之后不久，趋势科技就发现了 Android 平台 Yahoo! App 程序的漏洞，此漏洞可让黑客利用被入侵的 Yahoo! 帐号发送垃圾邮件。近日趋势科技发现了多个专门传播虚假药品网站链接或网络钓鱼网站链接的电子邮件。这一波垃圾邮件信息的签名部分有着“Sent from Yahoo! Mail on Android”的字样，而且信件的 Message-ID 栏显示有“androidMobile”字样。根据报导，其 IP 地址显示这些信息来自某些发展中国家的网络从业人员。某些专家依据这些证据猜测，这些垃圾邮件的发布者可能利用了被植入恶意程序的 Android 设备，不过 Google 驳斥了垃圾邮件是从 Android 僵尸网络发送的这种说法，并宣称应该是有人使用已感染的个人电脑，并在邮件中假冒移动设备的特征，试图躲避电子邮件过滤机制。无论垃圾邮件是从哪里发出的，用户依然必须小心这些垃圾邮件，因为他们仍具某些威胁性。用户如果点击这些链接，就会被引导到虚假药品网站，这些网站专门提供假的产品，甚至可能访问到钓鱼网站，用户会被要求提供自己的个人信息。因此请不要下载可疑邮件，或点击其中的链接。Android 用户必须尽量避免从非官方应用程序商店下载程序，因为这会增加下载到恶意应用的机会。

参考链接：<http://security.ctocio.com.cn/299/12401299.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的全称是国家计算机网络应急技术处理协调中心（英文简称是

CNCERT 或 CNCERT/CC) 成立于 1999 年 9 月, 是工业和信息化部领导下的国家级网络安全应急机构, 致力于建设国家级的网络安全监测中心、预警中心和应急中心, 以支撑政府主管部门履行网络安全相关的社会管理和公共服务职能, 支持基础信息网络的安全防护和安全运行, 支援重要信息系统的网络安全监测、预警和处置; 国家互联网应急中心在我国大陆 31 个省、自治区、直辖市设有分中心。

网址: [www.cert.org.cn](http://www.cert.org.cn)

邮箱: [vreport@cert.org.cn](mailto:vreport@cert.org.cn)

电话: 010-82990999