

## 信息安全漏洞周报

2014 年 4 月 21 日-2014 年 4 月 27 日

2014 年第 17 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 120 个，其中高危漏洞 35 个、中危漏洞 72 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 108 个。本周收录的漏洞中，已有 87 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 “Nagios Remote Plugin Executor 'nrpe.c' 远程代码执行漏洞”、“Xerox DocuShare 'dsweb/ResultBackgroundJobMultiple/' SQL 注入漏洞”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 6 家成员单位、合作伙伴及个人报送了本周收录的全部 120 个漏洞。报送情况如表 1 所示。其中，安天实验室、天融信、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、习科网络安全及多个白帽子向 CNVD 提交了 88 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   | 126    | 0      |
| 天融信     | 101    | 0      |
| 恒安嘉新    | 70     | 0      |
| 启明星辰    | 46     | 0      |
| 东软      | 3      | 0      |
| 绿盟科技    | 1      | 0      |
| 习科网络安全  | 58     | 58     |

|               |         |    |
|---------------|---------|----|
| CNCERT 广东分中心  | 8       | 8  |
| CNCERT 山西分中心  | 6       | 6  |
| CNCERT 安徽分中心  | 5       | 5  |
| CNCERT 吉林分中心  | 1       | 1  |
| CNCERT 广西分中心  | 1       | 1  |
| CNCERT 河北分中心  | 1       | 1  |
| CNCERT 江西分中心  | 1       | 1  |
| CNCERT 内蒙古分中心 | 1       | 1  |
| CNCERT 上海分中心  | 1       | 1  |
| 个人            | 5       | 5  |
| 报送总计          | 435     | 88 |
| 录入总计          | 120（去重） | 88 |

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Apple、Cisco、HP 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  | Apple        | 10   | 8%   |
| 2  | Cisco        | 6    | 5%   |
| 3  | HP           | 5    | 4%   |
| 4  | IBM          | 4    | 3%   |
| 5  | Wordpress    | 4    | 3%   |
| 6  | WebTitan     | 4    | 3%   |
| 7  | Freehelpdesk | 4    | 3%   |
| 8  | Django       | 3    | 3%   |
| 9  | Symantec     | 3    | 3%   |
| 10 | 其它           | 77   | 65%  |

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 120 个漏洞。其中应用程序漏洞 66 个，WEB 应用漏洞 26 个，操作系统漏洞 13 个，网络设备漏洞 9 个，安全产品漏洞 6 个。

|          |      |
|----------|------|
| 漏洞影响对象类型 | 漏洞数量 |
|----------|------|

|          |    |
|----------|----|
| 应用程序漏洞   | 66 |
| WEB 应用漏洞 | 26 |
| 操作系统漏洞   | 13 |
| 网络设备漏洞   | 9  |
| 安全产品漏洞   | 6  |

表 3 漏洞按影响类型统计表

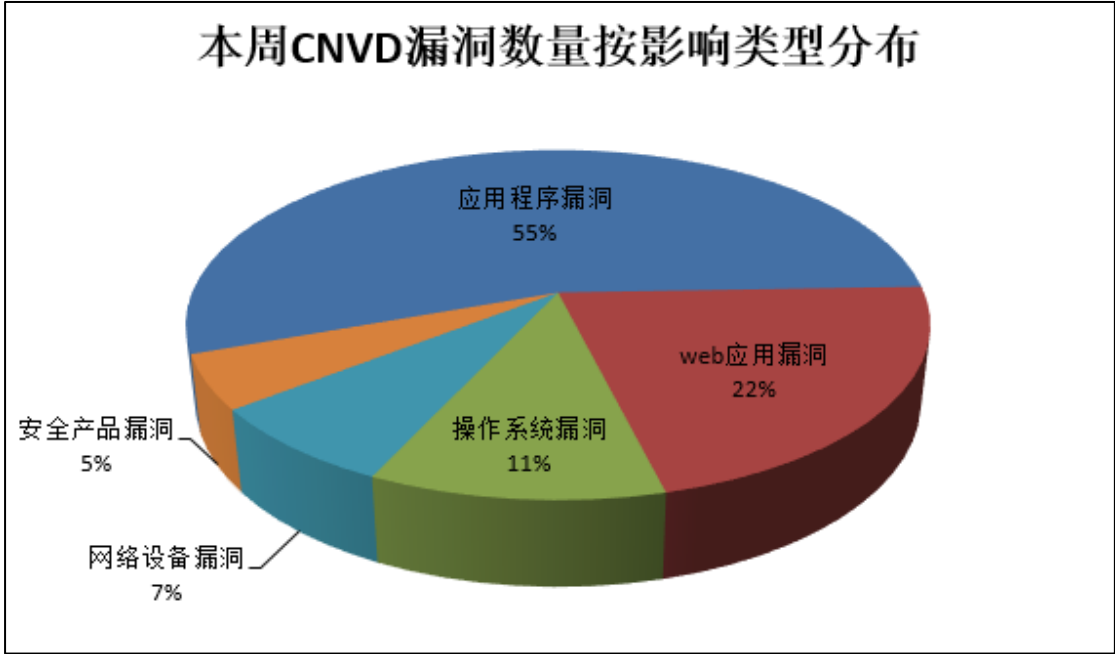


图 1 本周漏洞按影响类型分布

### 本周行业漏洞信息

本周，CNVD 收录了 11 个电信行业漏洞、2 个移动互联网行业漏洞、2 个工控系统行业漏洞（如下列表所示）。其中，“ZyXEL NBG-419N 路由器存在多个漏洞、ASUS RT-AC68U other RT series routers with firmware 任意命令执行漏洞”的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序。

| 行业 | 漏洞编号            | 漏洞标题                                                                | 危险等级 | 是否有补丁 |
|----|-----------------|---------------------------------------------------------------------|------|-------|
| 电信 | CNVD-2014-02538 | ASUS RT-Series Wireless Routers 'Advanced_System_Content.asp'信息泄露漏洞 | 中    | 是     |
| 电信 | CNVD-2014-02557 | ZyXEL NBG-419N 路由器存在多个漏洞                                            | 高    | 是     |
| 电信 | CNVD-2014-02560 | Cisco Network Registrar DHC Pv6 拒绝服务漏洞                              | 中    | 是     |
| 电信 | CNVD-2014-02621 | Teracom T2-B-Gawv1.4U10Y-BI 跨站请求伪造漏洞                                | 中    | 否     |

|       |                 |                                                              |   |   |
|-------|-----------------|--------------------------------------------------------------|---|---|
| 电信    | CNVD-2014-02623 | Juniper JunOS 'webauth_login.php ap_name'参数跨站脚本漏洞            | 中 | 否 |
| 电信    | CNVD-2014-02633 | Microsoft Internet Information Services CRLF 注入漏洞            | 中 | 否 |
| 电信    | CNVD-2014-02641 | Cisco IOS 存在未明确漏洞                                            | 中 | 是 |
| 电信    | CNVD-2014-02642 | Cisco IOS 拒绝服务漏洞（CNVD-2014-02642）                            | 中 | 是 |
| 电信    | CNVD-2014-02643 | Cisco IOS 拒绝服务漏洞（CNVD-2014-02643）                            | 中 | 是 |
| 电信    | CNVD-2014-02646 | ASUS RT-AC68U other RT series routers with firmware 任意命令执行漏洞 | 高 | 是 |
| 电信    | CNVD-2014-02647 | Cisco IOS 拒绝服务漏洞（CNVD-2014-02647）                            | 中 | 是 |
| 移动互联网 | CNVD-2014-02599 | AndExplorer And AndExplore rPro 远程目录遍历漏洞                     | 中 | 是 |
| 移动互联网 | CNVD-2014-02605 | 多个 Apple 产品安全绕过漏洞                                            | 中 | 是 |
| 工控系统  | CNVD-2014-02544 | Progea Movicon 信息泄露漏洞                                        | 中 | 是 |
| 工控系统  | CNVD-2014-02636 | Sixnet SixView Manager 目录遍历漏洞                                | 中 | 否 |

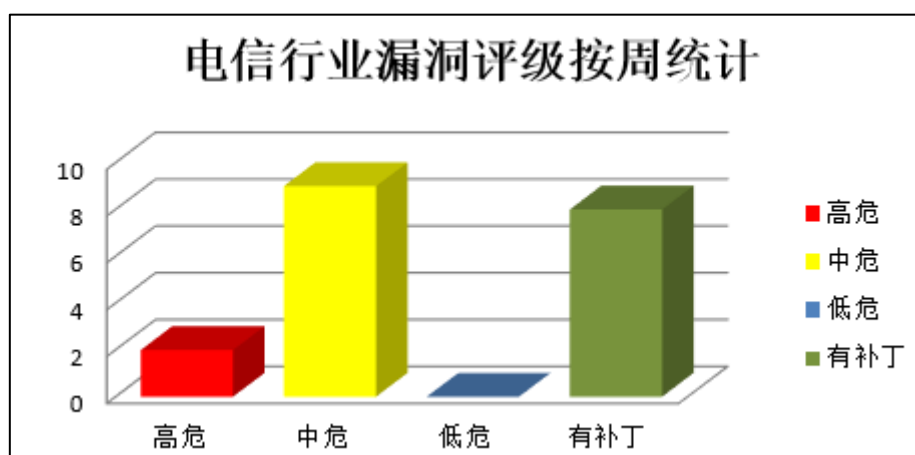


图 1 电信行业漏洞统计

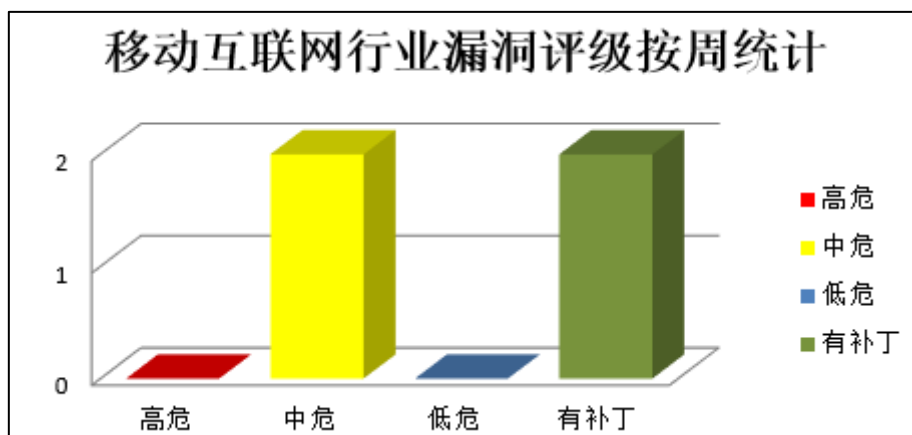


图 2 移动互联网行业漏洞统计

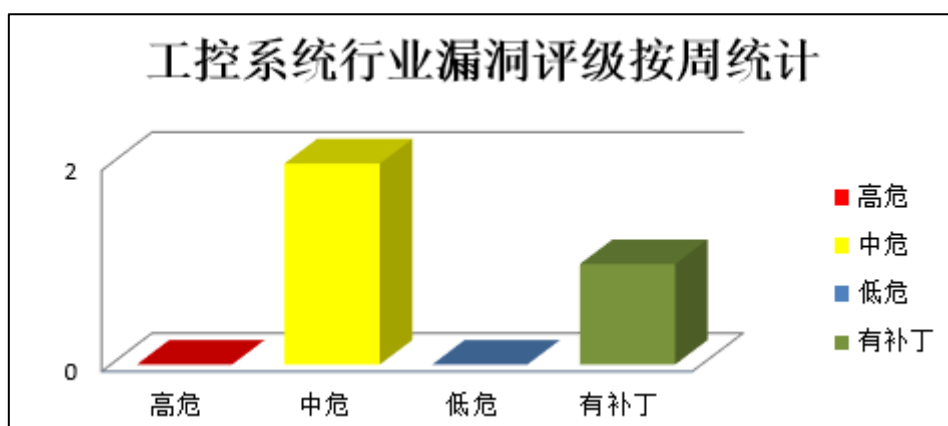


图 3 工控行业漏洞统计

## 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、Apple 产品安全漏洞

Apple Mac OS X 是一款苹果公司开发的操作系统。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Apple MAC OS X WindowServer 任意代码执行漏洞、Apple Mac OS X 远程拒绝服务漏洞、Apple Mac OS X 远程安全绕过漏洞、Apple MAC OS X ASLR 安全绕过漏洞、Apple MAC OS X URL 处理格式串漏洞。除“Apple MAC OS X ASLR 安全绕过漏洞、Apple MAC OS X URL 处理格式串漏洞”外，其余漏洞的综合评级均为“高危”。厂商已经发布了漏洞的修补程序。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-2014-02607>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02604>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02595>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02611>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02608>

## 2、HP 产品安全漏洞

HP NNMI 是一款网络服务的解决方案。HP Universal Configuration Management Database 是惠普公司的统一配置管理数据库应用。HP LoadRunner 是一款惠普公司开发的性能测试工具。本周，上述产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：HP Network Node Manager i (NNMi)远程代码执行漏洞、HP Universal Configuration Management Database 远程代码执行漏洞、HP Load Runner Virtual User Generator 远程代码执行漏洞。上述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-2014-02597>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02533>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02535>

## 3、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联网络操作系统。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 Network Registrar 为企业网络提供了一个灵活的命名和编址方案，以简化 IP 地址的管理。本周，上述产品被披露存在拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IOS 拒绝服务漏洞（CNVD-2014-02647、CNVD-2014-02643、CNVD-2014-02642）、Cisco Adaptive Security Appliance (ASA) SIP 远程拒绝服务漏洞、Cisco Network Registrar DHCPv6 拒绝服务漏洞。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网络安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02647>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02643>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02642>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02603>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02560>

## 4、Freehelpdesk 产品安全漏洞

Freehelpdesk 是一个桌面帮助系统，基于 Web 的接口，采用 PHP 开发。本周，该产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息或执行任意代码。

CNVD 收录的相关漏洞包括：Freehelpdesk 'key' GET 参数 SQL 注入漏洞、Freehelpdesk 'user\_id'参数 SQL 注入漏洞、Freehelpdesk 'email'参数存储跨站脚本漏洞、Freehelpdesk 'note\_body' POST 参数存储跨站脚本漏洞。其中，“Freehelpdesk 'key' GET 参数 SQL 注入漏洞、Freehelpdesk 'user\_id'参数 SQL 注入漏洞”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-2014-02592>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02593>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02591>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-02590>

## 5、Jzip 远程堆缓冲区溢出漏洞

Jzip 是一款免费的压缩解压软件。本周，Jzip 被披露存在一个综合评级为“高危”的堆缓冲区溢出漏洞。由于 Jzip 未能正确处理 Zip 文件，允许攻击者利用漏洞构建恶意文件，诱使用户解析，可使应用程序崩溃或执行任意代码。目前，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-2014-02615>

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-2014-02542 | Sfpagent Ruby Gem 远程命令注入漏洞                                    | 高    | Ruby Gem sfpagent 0.4.15 已经修复该漏洞，建议用户下载更新：<br><a href="http://rubygems.org/gems/sfpagent">http://rubygems.org/gems/sfpagent</a>                      |
| CNVD-2014-02580 | MODx Revolution 存在多个 SQL 注入漏洞                                 | 高    | MODX 2.2.14 已经修复该漏洞，建议用户下载更新：<br><a href="http://modx.com/blog/2014/04/04/revolution-2.2.14/">http://modx.com/blog/2014/04/04/revolution-2.2.14/</a> |
| CNVD-2014-02548 | libmms MMSH Server 应答堆缓冲区溢出漏洞                                 | 高    | libmms 0.6.4 已经修复该漏洞，建议用户下载更新：<br><a href="http://sourceforge.net/p/libmms/">http://sourceforge.net/p/libmms/</a>                                    |
| CNVD-2014-02547 | MicroWorld Technologies eScan Web Management 'pass'参数远程命令注入漏洞 | 高    | 暂无                                                                                                                                                   |
| CNVD-2014-02557 | ZyXEL NBG-419N 路由器存在多个漏洞                                      | 高    | 暂无                                                                                                                                                   |

|                 |                                             |   |                                                                                                                |
|-----------------|---------------------------------------------|---|----------------------------------------------------------------------------------------------------------------|
| CNVD-2014-02558 | vtiger CRM 密码重置安全限制绕过漏洞                     | 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：<br><a href="http://www.vtiger.com/">http://www.vtiger.com/</a>               |
| CNVD-2014-02566 | Cybozu Remote Service 拒绝服务漏洞                | 高 | Cybozu Remote Service 3.1.1 已经修复该漏洞，建议用户下载更新：<br><a href="http://www.cybozu.co.jp">http://www.cybozu.co.jp</a> |
| CNVD-2014-02617 | phpManufaktur/kitForm 'sorter.php' SQL 注入漏洞 | 高 | 暂无                                                                                                             |
| CNVD-2014-02571 | Qemu 'virt_load()'缓冲区溢出漏洞                   | 高 | 暂无                                                                                                             |
| CNVD-2014-02588 | KnowledgeTree 'mdownload.php' SQL 注入漏洞      | 高 | 用户可联系供应商获得补丁信息：<br><a href="https://www.knowledgetree.com">https://www.knowledgetree.com</a>                   |

表 3 部分高危漏洞列表

小结：本周，Apple 被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。此外，HP、Cisco、Freehelpdesk 集中披露多款产品存在多个漏洞，攻击者可利用漏洞获取敏感信息、执行任意代码或发起拒绝服务攻击。另外，Jzip 被披露存在一个高危零日漏洞，攻击者可利用漏洞构建恶意文件，诱使用户解析，可使应用程序崩溃或执行任意代码。CNVD 已经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、Oracle 修补 WebLogic Server 产品漏洞

Oracle Weblogic Server 是应用程序服务器。

本周，Oracle 修补了上述产品存在的未明远程漏洞，避免远程攻击者利用漏洞发起其他攻击可影响系统的机密性、完整性、可用性，暂时没有详细的漏洞细节。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网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/45080>

## 本周要闻速递

### 1. “越狱” iPhone 中存恶意代码 被疑来自中国

网易科技讯 4 月 22 日消息，据国外媒体报道，德国手机安全商 SektionEins 日前表示，部分“越狱”的 iOS 设备中存在一款名为“unfold baby panda”（展开的熊猫宝宝）的恶意程序。该程序可窃取用户的帐号及密码。并根据德国手机安全商 SektionEins 所公布的信息，被感染文件的数字签名属于一位来自中国的 iPhone 开发者——Wang Xin。此外，该恶意程序总是试图将窃取到的苹果帐号及密码以明文形式不断向一个中国 IP（23.88.10.4）发送。因此不禁让人怀疑，此恶意程序或是源自中国——而为了暗示这样的出身，网友也给该恶意程序取名为“unfold baby panda”。

参考链接：<http://tech.163.com/14/0422/04/9QDJBREB000915BE.html>

## 2. Struts2 再曝安全漏洞

Struts2 再次爆出安全漏洞。国外安全研究人员日前发现，Apache Struts2 在处理 CVE-2014-0094 的漏洞补丁中存在缺陷，会被轻易绕过，可导致任意命令执行。黑客进而能够窃取到网站数据，或者对网站进行 DDoS 攻击。截至目前，Apache 官方仍未发布该漏洞修复方案。

参考链接：[http://www.cb.com.cn/gongsikuaixun/2014\\_0424/1056116.html](http://www.cb.com.cn/gongsikuaixun/2014_0424/1056116.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

国家计算机网络应急技术处理协调中心（简称“国家互联网应急中心”，英文简称是 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，为非政府非盈利的网络安全技术中心，是我国网络安全应急体系的核心协调机构。

作为国家级应急中心，CNCERT 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

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