

信息安全漏洞周报

2015 年 06 月 01 日-2015 年 06 月 07 日

2015 年第 23 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 112 个，其中高危漏洞 27 个、中危漏洞 73 个、低危漏洞 12 个。上述漏洞中，可利用来实施远程攻击的漏洞有 100 个。本周收录的漏洞中，已有 89 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。其中互联网上出现“i.FTP 'schedule.xml'处理缓冲区溢出漏洞”、“Clickheat 命令执行漏洞”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 6 家成员单位、合作伙伴及个人报送了本周收录的全部 112 个漏洞。报送情况如表 1 所示。其中，奇虎、启明星辰、安天实验室、天融信等单位报送数量较多。此外，CNCERT 各分中心、乌云、漏洞盒子、四川大学信息安全研究所、汉柏科技有限公司及白帽子向 CNVD 提交了 659 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎	354	354
启明星辰	133	0
安天实验室	123	0
天融信	109	0
恒安嘉新	89	0
绿盟科技	13	0

High-Tech Bridge Security Research Lab	1	1
乌云	248	248
漏洞盒子	6	6
四川大学信息安全研 究所	4	4
汉柏科技有限公司	2	2
CNCERT 安徽分中心	4	4
CNCERT 甘肃分中心	4	4
CNCERT 福建分中心	2	2
CNCERT 河南分中心	1	1
个人	33	33
报送总计	1126	659
录入总计	112（去重）	659

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、WordPress、IBM 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	15	13%
2	WordPress	13	12%
3	IBM	8	7%
4	Aruba Networks	6	5%
5	PHP	5	4%
6	SAP	5	4%
7	D-Link	4	4%
8	Apache	3	3%
9	Red Hat	2	2%
10	其他	51	46%

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 112 个漏洞。其中应用程序漏洞 69 个，WEB 应用漏洞 19 个，网络设备漏洞 15 个，操作系统漏洞 4 个，数据库漏洞 3 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	69
WEB 应用漏洞	19
网络设备漏洞	15
操作系统漏洞	4
数据库漏洞	3
安全产品漏洞	2

表 3 漏洞按影响类型统计表

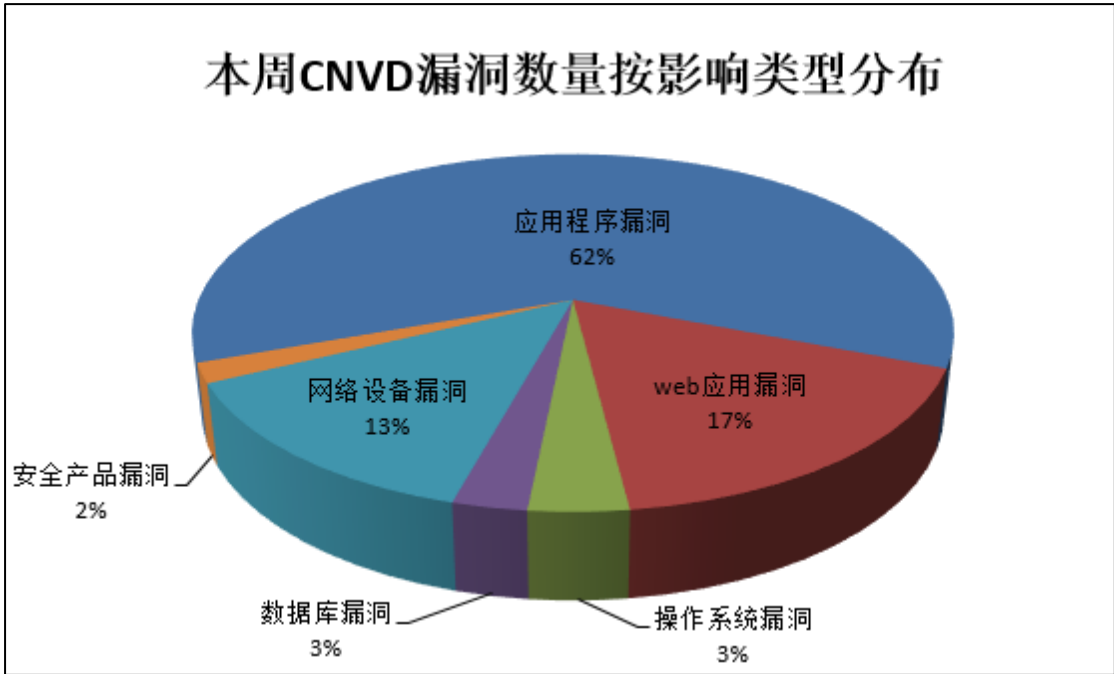


图 1 本周漏洞按影响类型分布



本周行业漏洞信息

本周，CNVD 收录了 6 个电信行业漏洞，2 个移动互联网行业，1 个工控系统行业漏洞（如下图表所示）。其中，“AVM Fritz!Box 任意命令执行漏洞、Cisco AnyConnect Secure Mobility Client Posture 模块权限提升漏洞、SAP Afaria 信息泄露漏洞”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-2015-03595	Cisco AnyConnect Secure Mobility Client 权限提升漏洞（CNVD-2015-03595）	中	是
电信	CNVD-2015-03563	AVM Fritz!Box 任意命令执行漏洞	高	是
电信	CNVD-2015-03500	Cisco AnyConnect Secure Mobility Client Posture 模块权限提升漏洞	高	是
电信	CNVD-2015-03501	IBM Business Process Manager 跨站脚本漏洞（CNVD-2015-03501）	中	是
电信	CNVD-2015-03489	IBM WebSphere Portal 开放重定向漏洞（CNVD-2015-03489）	中	是
电信	CNVD-2015-03488	IBM Business Process Manager 跨站脚本漏洞（CNVD-2015-03488）	低	是
移动互联网	CNVD-2015-03580	SAP Afaria 信息泄露漏洞	高	是
移动互联网	CNVD-2015-03503	Apache Cordova For Android 安全绕过漏洞	中	是
工控系统	CNVD-2015-03559	Rockwell Automation RSView32 信息泄露漏洞	中	是

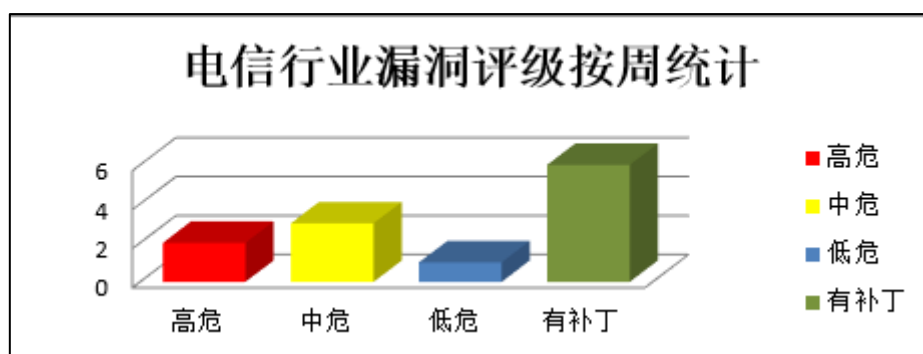


图 1 电信行业漏洞统计

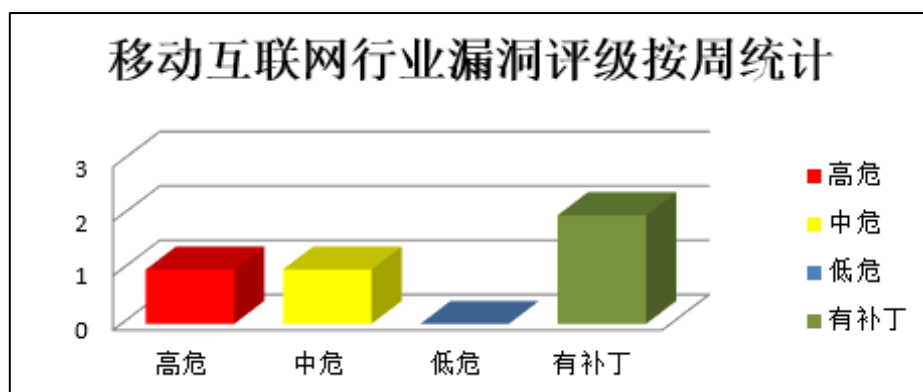


图 2 移动互联网行业漏洞统计

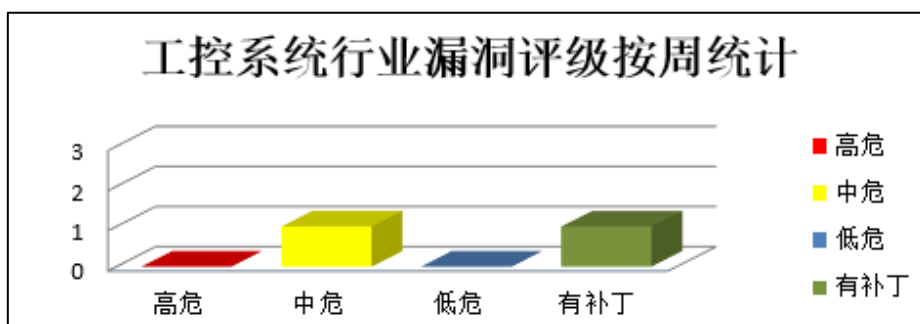


图3 工控系统行业漏洞统计

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、Cisco 产品安全漏洞

Cisco Headend Digital Broadband Delivery System 是一套数字宽带传输系统；Cisco AnyConnect Secure Mobility Client 是思科下一代 VPN 客户端；Cisco Unified MeetingPlace 是一套多媒体会议解决方案；Cisco WLC 负责全系统的无线 LAN 功能，例如安全策略、入侵保护、RF 管理，服务质量和移动性。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取敏感信息，提升权限，发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco AnyConnect Secure Mobility Client 权限提升漏洞(CNVD-2015-03595)、Cisco Unified MeetingPlace WEB 接口任意文件读取漏洞、Cisco Headend System Release UDP 拒绝服务漏洞、Cisco Headend System Release Digital Broadband Delivery System CRLF 注入漏洞、Cisco Conductor for Videoscape 和 Cisco Headend System Release 任意 cookie 注入漏洞、Cisco Headend System Release 敏感信息泄露漏洞、Cisco AnyConnect Secure Mobility Client Posture 模块权限提升漏洞、Cisco Wireless LAN Controller TCP 流量处理拒绝服务漏洞。其中，“Cisco AnyConnect Secure Mobility Client Posture 模块权限提升漏洞”的综合评级为“高危”。目前，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-2015-03595>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03557>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03561>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03568>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03566>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03565>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03500>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03508>

2、Aruba 产品安全漏洞

Aruba Networks ClearPass Policy Manager 是基于角色及设备的进行网络访问控制的高级策略管理平台。本周，该产品被披露存在跨站脚本、目录遍历、SQL 注入和远程代码执行漏洞。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：Aruba Networks CPPM 跨站脚本漏洞（CNVD-2015-03502）、Aruba Networks CPPM SQL 注入漏洞、Aruba Networks CPPM 远程代码执行漏洞、Aruba Networks CPPM 目录遍历漏洞（CNVD-2015-03506、CNVD-2015-03507）、Aruba Networks CPPM 跨站脚本漏洞（CNVD-2015-03509）。其中，“Aruba Networks CPPM 远程代码执行漏洞、Aruba Networks CPPM 目录遍历漏洞（CNVD-2015-03506）”的综合评级均为“高危”。目前，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-2015-03502>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03504>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03505>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03506>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03507>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03509>

3、D-Link 产品安全漏洞

D-Link DNR-326 是友讯（D-Link）公司的一款 NAS 网络存储器产品。本周，多个 D-Link 产品被披露存在多个安全漏洞。攻击者可利用漏洞获取绕过安全限制，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：D-Link DNR-326 身份验证绕过漏洞、多个 D-Link 产品存在多个认证绕过漏洞、多个 D-Link 产品缓冲区溢出漏洞、多个 D-link 产品安全绕过漏洞。其中，“多个 D-Link 产品缓冲区溢出漏洞”的综合评级均为“高危”。目前，除“多个 D-link 产品安全绕过漏洞”外，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-2015-03606>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03605>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03604>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03603>

4、WordPress 插件安全漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。本周，该产品多个插件被披露存在跨站请求伪造、跨站脚本和远程代码执行漏洞。攻击者可利用漏洞获取敏感信息、进行跨站攻击或执行任意代码。

CNVD 收录的相关漏洞包括:WordPress 插件 WPS Hide Login 跨站请求伪造漏洞、WordPress Anti-Malware and Brute-Force Security by ELI 插件存在多个漏洞、WordPress NextScripts: Social Networks Auto-Poster HTML 注入漏洞、WordPress 插件 Roomcloud 'roomcloud.php'存在多个跨站脚本漏洞、WordPress 插件 church_admin 跨站脚本漏洞、WordPress RevSlider 文件上传远程执行代码漏洞、WordPress 插件 Free Counter 跨站脚本漏洞、WordPress 插件 WP Fast Cache 跨站脚本漏洞。其中“WordPress Anti-Malware and Brute-Force Security by ELI 插件存在多个漏洞、WordPress RevSlider 文件上传远程执行代码漏洞”的综合评级为“高危”。除“WordPress 插件 Free Counter 跨站脚本漏洞”、“WordPress 插件 WP Fast Cache 跨站脚本漏洞”外,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-2015-03609>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03611>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03610>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03516>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03493>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03510>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03492>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-03613>

5、Apple iOS CoreText Unicode 拒绝服务漏洞

Apple iOS 是一款由苹果公司开发,应用于智能设备上的操作系统。本周,Apple iOS 被披露存在综合评级为“高危”的拒绝服务漏洞。允许远程攻击者利用特制的 Unicode 文本使应用程序崩溃或重启。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-2015-03517>

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-2015-03598	ResourceSpace 本地 PHP 文件包含漏洞	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://svn.montala.com/websvn/revision.php?repname=ResourceSpace&path=%2F&rev=6640&peg=6738
CNVD-2015-03589	FusionForge Git 插件存在漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息: https://fusionforge.org/forum/forum.php?forum_id=41

CNVD-2015-03622	NetApp OnCommand Workflow Automation 远程代码执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://kb.netapp.com/support/index?page=content&id=9010037
CNVD-2015-03599	Arcserve Unified Data Protection 存在多个目录遍历漏洞	高	目前厂商已经发布升级补丁/版本以修复这个安全问题，请用户及时下载更新： http://documentation.arcserve.com/Arcserve-UDP/Available/V5/ENU/Bookshelf_Files/HTML/Update%204/UDP_Update4_ReleaseNotes.html
CNVD-2015-03618	util-linux Package 'hwclock(8)'本地权限提升漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： https://www.kernel.org/pub/linux/utils/util-linux/
CNVD-2015-03593	Acoustica Pianissimo 'id'缓冲区溢出漏洞	高	暂无
CNVD-2015-03581	SAP ASE Database Platform 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： https://service.sap.com/sap/support/notes/2152278
CNVD-2015-03560	IBM PowerVC 权限提升漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www-01.ibm.com/support/docview.wss?uid=swg1IT08806
CNVD-2015-03563	AVM Fritz!Box 任意命令执行漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.fritzbox.eu/en/index.php
CNVD-2015-03517	Apple iOS CoreText Unicode 拒绝服务漏洞	高	暂无

表 3 部分高危漏洞列表

小结：本周，Cisco 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，提升权限，发起拒绝服务攻击。此外，Aruba、D-Link、WordPress 多款产品被披露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、进行跨站攻击，绕过安全限制，执行任意代码或发起拒绝服务攻击。另外，Apple iOS 被披露存在一个高危零日漏洞，攻击者利用特制的 Unicode 文本使应用程序崩溃或重启。建议相关用户应随时关注上述厂商主页，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、HP 修补多个产品漏洞

HP ThinPro Linux 和 HP Smart Zero Core 都是美国惠普（HP）公司的操作系统；HP SDN VAN Controller devices 是一套提供开源联网技术网络功能的统一控制设备。

本周，HP 修补了上述产品存在的本地权限提升、未授权访问和拒绝服务漏洞，避免攻击者利用漏洞获取未授权的访问权限或发起拒绝服务攻击。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/59342>

<http://www.cnvd.org.cn/patchInfo/show/59109>

本周要闻速递

1. 苹果发布 Mac 电脑安全补丁修正 20 多处漏洞

苹果电脑发布了 Mac 操作系统 X 的安全补丁，修正了包括网页浏览器以及电子邮件功能存在的安全隐患的 20 多处安全漏洞。而苹果 Mac 电脑的安全问题，在仅仅十几天的时间，Mac 操作系统就发现了两款蠕虫病毒和两个安全漏洞，这样的严重问题，早已引起了业界的广泛关注。对于这次发布的 Mac 操作系统 X 的安全补丁，主要是对 Safari 浏览器以及苹果 Mail 电子邮件软件进行了升级，同时也对苹果即时通讯软件 iChat 作出了修正，这样一来，用户就不会再受到以前爆发出的 Leap A pest 病毒的侵害。据称，该隐患在上周被安全专家所发现；而利用这些安全漏洞，黑客可以成功的入侵 Mac 电脑，从而对系统进行远程操纵。苹果透露此次的补丁，还修正了 PHP 脚本程序语言中存在的四个问题、苹果字典服务中的两个问题，以及 FileVault 安全存储功能中的一个 Bug。在浏览器方面，除了之前发现的漏洞以外，苹果此次发布的补丁还修正了另外四个未被公布的漏洞。据称，此次苹果发布的补丁版本号为 Security Update 2006 - 001，可以通过苹果网站进行下载，或者直接安装苹果 Mac 操作系统 X 升级补丁。

参考链接：<http://www.thethirdmedia.com/Article/200607/show42905c7p1.html>

2. SOHO 无线路由器再曝漏洞可被远程攻击

近日，作为路由器重要的芯片提供商 Realtek(瑞昱)就被曝出存在 SDK(软件开发工具包)方面的重要漏洞。目前这个编号为 CVE-2014-8361 的 Realtek SDK 远程代码执行漏洞已被安全研究人员公开，并有安全项目组将该漏洞在通用安全漏洞评分系统(CVSS)中被评为最高级别的 10 分。瑞昱 miniigd SOAP 服务器上存在一个严重缺陷。由于未能在执行系统调用前清理用户数据，导致在处理 NewInternalClient 请求时出现问题。而由 Realtek 推出的所有用于开发 RTL81xx 系列网卡驱动的软件开发工具包均受影响，包括有众多使用 RTL81xx 芯片组的供应商设备也存在这一问题。目前尚不清楚有多少商用级别和家用级别的无线路由器受此影响，但研究者认为所有使用 Realtek SDK miniigb 二进制的设备都存在安全隐患。其中包括 TP-Link、D-Link、趋势网络(TRENDnet)等品

牌产品。

参考链接: <http://it.szonline.net/network/512302/664409318189b.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

邮箱: vreport@cert.org.cn

电话: 010-82990999