

信息安全漏洞周报

2017 年 10 月 09 日-2017 年 10 月 15 日

2017 年第 42 期

本周漏洞态势研判情况

本周信息安全漏洞威胁整体评价级别为**高**。

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 219 个，其中高危漏洞 88 个、中危漏洞 115 个、低危漏洞 16 个。漏洞平均分为 6.38。本周收录的漏洞中，涉及 0day 漏洞 39 个（占 18%），其中互联网上出现“Vacron NVR 设备远程命令执行漏洞、Joomla! 组件 Ajax Quiz SQL 注入漏洞”零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 818 个。此外，本周微软漏洞补丁日发布修复了 Microsoft Windows SMB Server 远程执行代码漏洞，该漏洞影响版本范围跨度较大，一旦漏洞细节披露，将造成极为广泛的攻击威胁，可导致诱发 APT 攻击。

CNVD 收录漏洞近 10 周平均分分布图

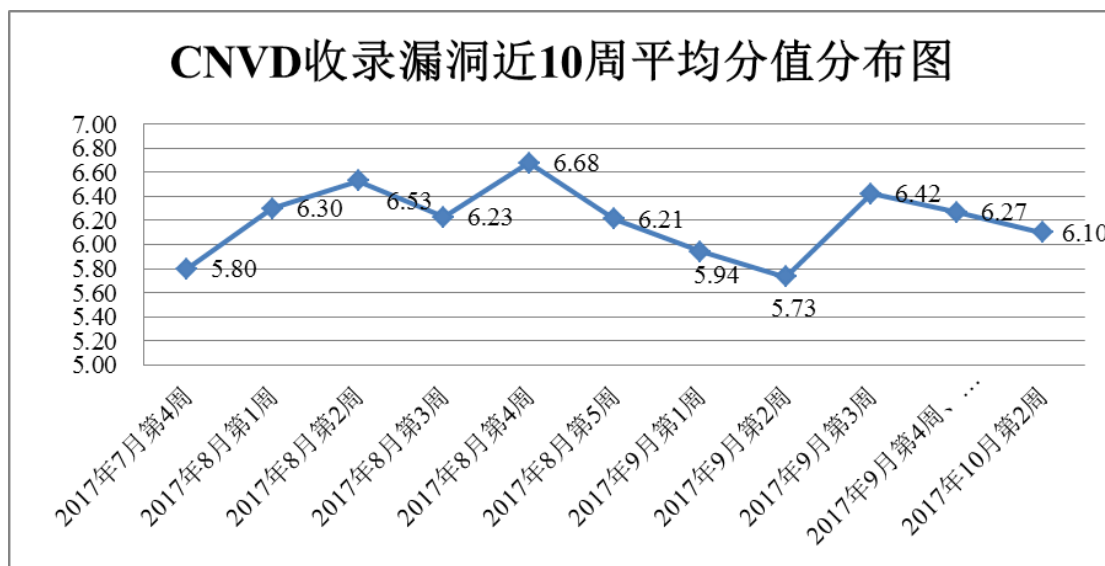


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，华为技术有限公司、安天实验室、天融信、北京

数字观星科技有限公司、恒安嘉新等单位报送数量较多。四川虹微技术有限公司（子午攻防实验室）、中新网络信息安全股份有限公司、深圳市鼎安天下信息科技有限公司、福建榕基软件股份有限公司、广州软云计算机科技有限公司、江苏金盾检测技术有限公司、北京长亭科技有限公司及其他个人白帽子向 CNVD 提交了 818 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
华为技术有限公司	258	0
H3C	236	0
安天实验室	222	0
天融信	162	3
漏洞盒子	200	200
360 网神	124	124
北京数字观星科技有限公司	119	0
恒安嘉新	117	0
启明星辰	75	3
中国电信集团系统集成有限责任公司	62	7
杭州安恒信息技术有限公司	50	0
绿盟科技	38	0
厦门服云信息科技有限公司	36	1
北京知道创宇信息技术有限公司	4	0
北京无声信息技术有限公司	2	0
西安四叶草信息技术有限公司	1	1
四川虹微技术有限公司 （子午攻防实验室）	43	43
中新网络信息安全股份有限公司	17	17

深圳市鼎安天下信息科技有限公司	13	13
福建榕基软件股份有限公司	2	2
广州软云计算科技有限公司	1	1
江苏金盾检测技术有限公司	1	1
北京长亭科技有限公司	1	1
CNCERT 吉林分中心	3	3
CNCERT 广东分中心	3	3
CNCERT 上海分中心	2	2
CNCERT 河北分中心	1	1
CNCERT 浙江分中心	1	1
个人	391	391
报送总计	2185	818

表 1 漏洞报送情况统计表



本周漏洞按类型和厂商统计

本周，CNVD 收录了 219 个漏洞。其中应用程序漏洞 168 个，操作系统漏洞 23 个，网络设备漏洞 13 个，web 应用漏洞 12 个，安全产品漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	168
操作系统漏洞	23
网络设备漏洞	13
web 应用漏洞	12
安全产品漏洞	3

表 2 漏洞按影响类型统计表

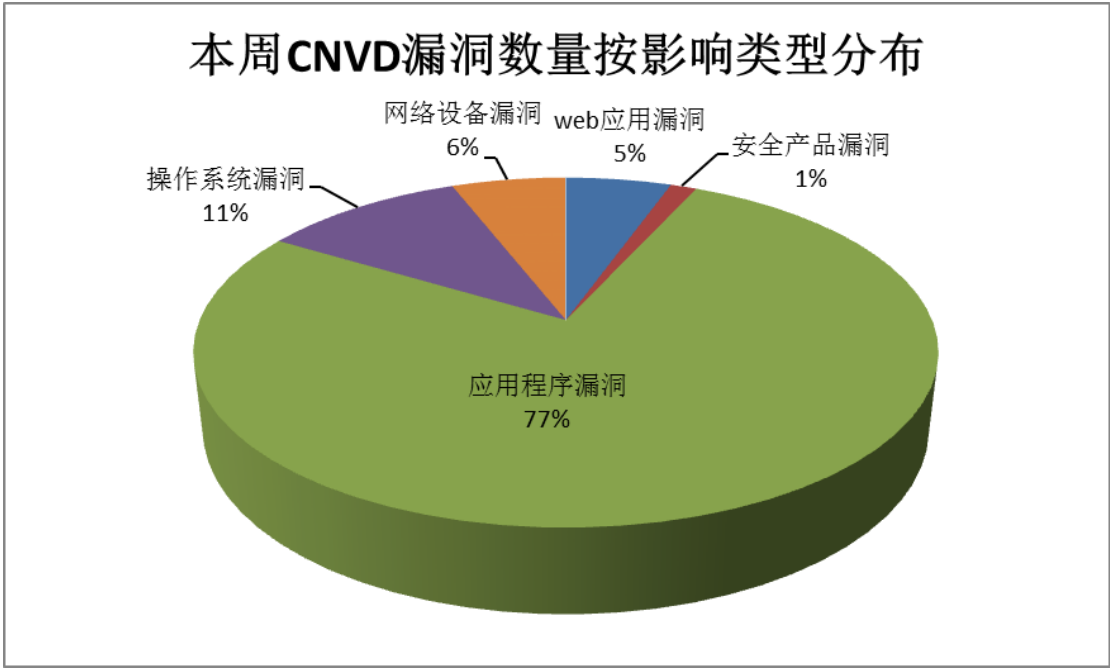


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Tcpdump、Microsoft、Oracle 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Google	14	6%
2	IBM	9	4%
3	SAP	9	4%
4	GNU	8	4%
5	Atlassian	7	3%
6	WordPress	6	3%
7	NexusPHP	6	3%
8	Cisco	5	2%
9	ProMinent	5	2%
10	其他	150	69%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 11 个电信行业漏洞，25 个移动互联网行业漏洞，12 个工控系统行业漏洞（如下图所示）。其中，“SCisco IOS XE Software 安全绕过漏洞、Apache Tomcat 远程代码执行漏洞（CNVD-2017-30092）、NoviFlow NoviWare 和 NoviSwitch 设

备远程代码执行漏洞、多款 Apple 产品 WebKit 组件内存破坏漏洞 (CNVD-2017-29710)、GE CIMPLICITY 栈缓冲区溢出漏洞”等漏洞的综合评级为“高危”。相关厂商已经发布了上述漏洞的修补程序，请参照 CNVD 相关行业漏洞库链接。

电信行业漏洞链接：<http://telecom.cnvd.org.cn/>

移动互联网行业漏洞链接：<http://mi.cnvd.org.cn/>

工控系统行业漏洞链接：<http://ics.cnvd.org.cn/>

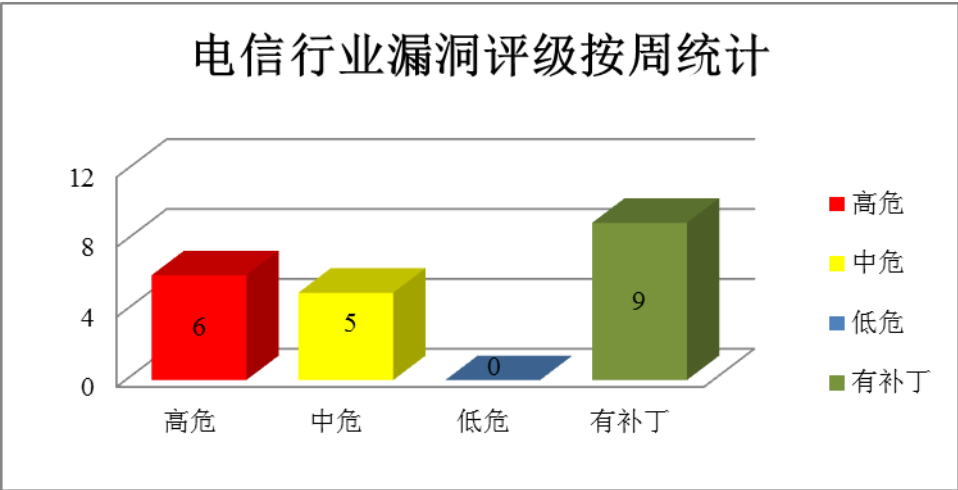


图 3 电信行业漏洞统计

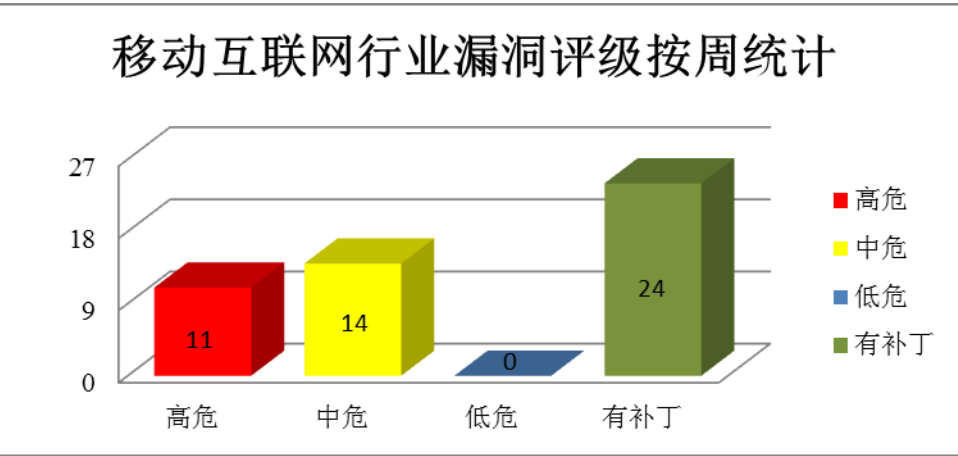


图 4 移动互联网行业漏洞统计

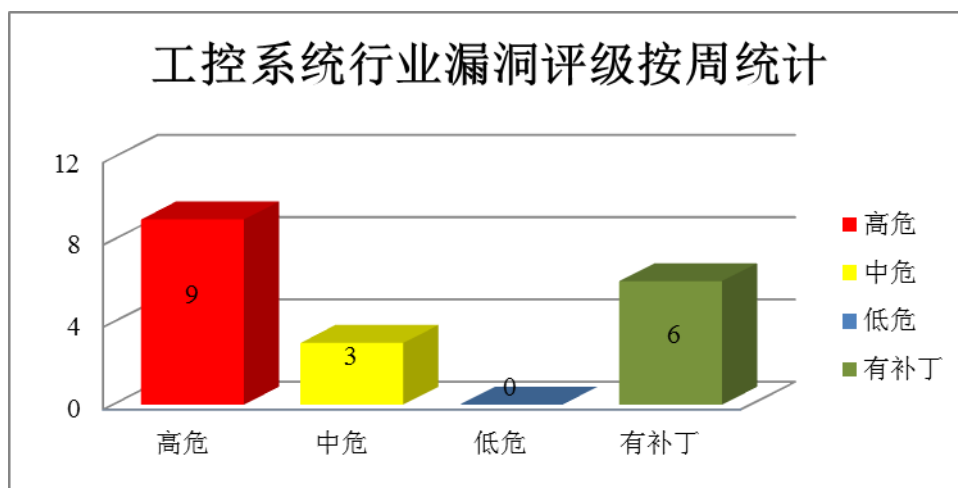


图 5 工控系统行业漏洞统计

本周重要漏洞安全告警

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

Microsoft Windows 是美国微软公司发布的一系列操作系统。Sever Message Block 是其中的一个为计算机提供身份验证用以访问服务器上打印机和文件系统的组件。Microsoft Office 一款办公软件套件产品。本周，上述产品被披露存在内存破坏和远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Windows SMB Server 远程代码执行漏洞、Microsoft Office 内存破坏漏洞（CNVD-2017-29849）。上述漏洞的综合评级为“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-2017-29681>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-29849>

2、DNSmasq 产品安全漏洞

DNSmasq 是一个小巧且方便地用于配置 DNS 和 DHCP 的工具。本周，该产品被披露存在拒绝服务、信息泄露和任意代码执行漏洞，攻击者可利用漏洞执行任意代码、泄露敏感信息或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：DNSmasq 拒绝服务漏洞（CNVD-2017-29272、CNVD-2017-29273、CNVD-2017-29274）、DNSmasq 任意代码执行漏洞、DNSmasq 任意代码执行漏洞（CNVD-2017-29276、CNVD-2017-29277）、DNSmasq 信息泄露漏洞。上述漏洞的综合评级为“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-2017-29272>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-29273>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-29274>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-29278>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-29276>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-29277>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-29275>

3、Google 产品安全漏洞

Android 是美国谷歌公司的一套以 Linux 为基础的开源操作系统。Media framework (libstagefright)是其中的一个用于多媒体开发的硬解码支持框架。Libraries 是其中的一个函数库。本周，上述产品被披露存在权限提升和远程代码执行漏洞，攻击者可利用漏洞提升权限或执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Framework ui framework 权限提升漏洞、Google Android Libraries 远程代码执行漏洞、Google Android Libraries 远程代码执行漏洞（CNVD-2017-30039）、Google Android Media framework audio hal 权限提升漏洞、Google Android Media framework libhevc 远程代码执行漏洞、Google Android Media framework libmpeg2 远程代码执行漏洞、Google Android Media framework libstagefright 远程代码执行漏洞、Google Android media framework 权限提升漏洞（CNVD-2017-30024）。上述漏洞的综合评级为“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-2017-29906>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30040>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30039>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-29904>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-29909>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-29907>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-29908>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30024>

4、GNU 产品安全漏洞

GNU Binutils 是一组用于创建和管理二进制程序、对象文件、库、配置文件数据及程序集源代码的编程工具。GNU Binutils 是 GNU 计划开发的一组编程语言工具程序。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：GNU Binutils Binary File Descriptor 库拒绝服务漏洞、GNU Binutils 拒绝服务漏洞（CNVD-2017-30067、CNVD-2017-30068、CNVD-2017-30069、CNVD-2017-30072、CNVD-2017-30073、CNVD-2017-30074、CNVD-2017-30075）。其中“GNU Binutils 拒绝服务漏洞（CNVD-2017-30072）”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-2017-29734>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30067>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30068>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30069>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30072>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30073>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30074>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-30075>

5、LAVA Computer MFG Ether-Serial Link 认证绕过漏洞

Ether-Serial Link 是 LAVA Computer MFG 公司的一款以太网串行链路设备。本周，LAVA Computer MFG 被披露存在认证绕过漏洞，具有相同 IP 地址的攻击者可利用漏洞通过访问特定的资源定位符来绕过身份验证。目前，厂商尚未发布漏洞修补程序。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-2017-29694>

更多高危漏洞如表 4 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-2017-29435	SAP NetWeaver 存在未明 SQL 注入漏洞	高	用户可联系供应商获得补丁信息： https://help.sap.com/viewer/p/SAP_NETWEAVER
CNVD-2017-29449	X.Org libXfont catalogue.c 文件缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.x.org/
CNVD-2017-29540	SaltStack Salt 目录遍历漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://bugzilla.redhat.com/show_bug.cgi?id=1482006
CNVD-2017-29544	Unity Editor 远程代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://unity3d.com/cn/security#issues
CNVD-2017-29917	ArcGIS Server 远程命令执行漏洞	高	用户可联系供应商获得补丁信息： http://server.arcgis.com/zh-cn/
CNVD-2017-29974	Envitech Ltd EnviDAS Ultimate 身份验证绕过漏洞	高	用户可联系供应商获得补丁信息： https://ics-cert.us-cert.gov/advisories/ICSA-17-285-03
CNVD-2017-30075	BMC Patrol 权限提升漏洞	高	用户可参考如下厂商提供的安全补丁

7-30026			以修复该漏洞： http://www.bmc.com/
CNVD-2017-30046	Apache Pony Mail 安全绕过漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://markmail.org/message/jy7o23cppny26icu
CNVD-2017-30072	GNU Binutils 拒绝服务漏洞(CNVD-2017-30072)	高	厂商已发布漏洞修复程序，请及时关注更新： https://sourceware.org/bugzilla/show_bug.cgi?id=22191
CNVD-2017-30085	FileRun 远程 SQL 注入漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： https://docs.filerun.com/updates

表 4 部分重要高危漏洞列表

小结：本周，Microsoft 存在内存破坏和远程代码执行漏洞，攻击者可利用漏洞执行任意代码。此外，DNSmasq、Google、GNU 多款产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息、执行任意代码或发起拒绝服务攻击等。另外，LAVA Computer MFG 被披露存在认证绕过漏洞，具有相同 IP 地址的攻击者可利用漏洞通过访问特定的资源定位符来绕过身份验证。建议相关用户随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周漏洞要闻速递

1. 海洋 CMS (SEACMS) 0day 漏洞预警

海洋 CMS 是一套专为不同需求的站长而设计的视频点播系统，在影视类 CMS 中具有很高的市场占有率。目前海洋 CMS (SEACMS) 的 0day 已经被大规模运用，而且攻击者使用自动化攻击脚本对全网 SEACMS 进行搜索并实施自动攻击。截至 2017.10.9，SEACMS 仍然未发布该漏洞的补丁。建议 SEACMS 用户立即安装云锁并开启文件防上传功能，可暂时避免被自动化程序攻击。

参考链接：<http://www.freebuf.com/vuls/150042.html>

2. GDI 信息泄露漏洞 CVE-2017-11816

这个漏洞主要是因为 GDI32 在处理 metafile META_DIBSTRETCHBLT record 时候内存拷贝，越界读，导致的信息泄露漏洞。该漏洞可以在 wordpad outlook 直接触发，如果想在 edge, ie 中触发需要修改一下 poc 中的某些数据，把十六进制数据贴到 010editor，然后保存成 wmf 文件格式即可。

参考链接：<http://www.freebuf.com/vuls/150457.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

邮箱：vreport@cert.org.cn

电话：010-82991537