国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 03 月 13 日-2017 年 03 月 19 日 **2017 年第 12 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 109 个，其中高危漏洞 39 个、中危漏洞 55 个、低危漏洞 15 个。漏洞平均分值为 5.95。本周收录的漏洞中，涉及 0day 漏洞 73 个（占 38%）。其中互联网上出现“WePresent WiPG-1500 后门漏洞、WordPress Adminer 插件允许公共管理(本地)数据库登录漏洞”等零日代码攻击漏洞。此外，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 408 个，与上周（724 个）环比下降 44%。

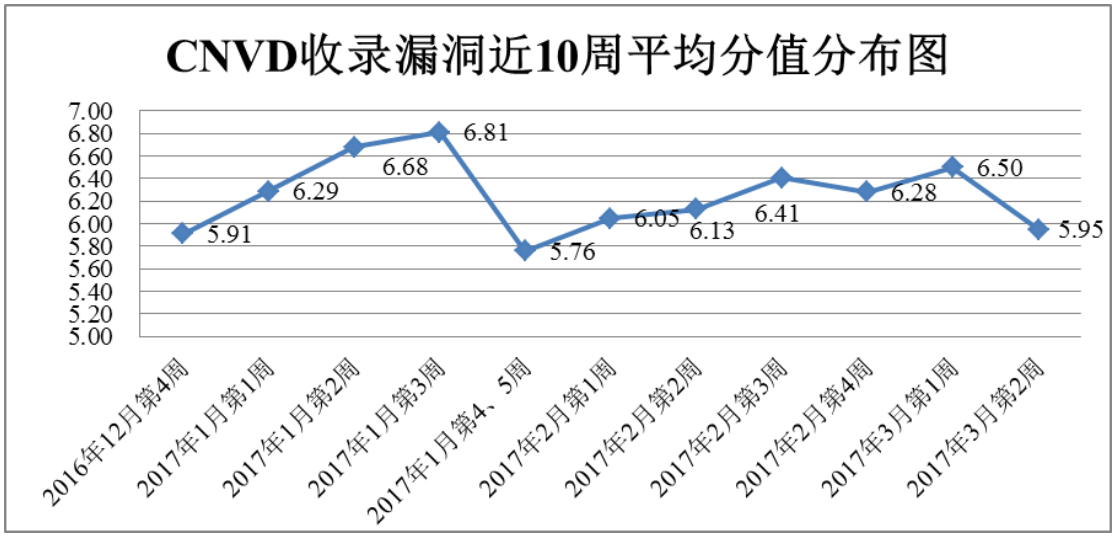

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 17 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 109 个漏洞。报送情况如表 1 所示。其中，蓝盾信息安全技术有限公司、安天实验室、天融信、华为技术有限公司、绿盟科技等单位报送数量较多。漏洞盒子、广西鑫瀚科技有限公司、清远职业技术学院及其他个人白帽子向 CNVD 提交了 408 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
蓝盾信息安全技术有限公司	326	0
安天实验室	161	0
天融信	141	1
华为技术有限公司	90	0
绿盟科技	72	0
H3C	58	1
中国电信集团系统集成有限责任公司	30	0
恒安嘉新	22	0
杭州安恒信息技术有限公司	22	0
安全狗	22	4
卫士通信息产业股份有限公司	15	0
阿里云计算有限公司	13	0
知道创宇	13	0
北京数字观星科技有限公司	5	0
深圳市深信服电子科技有限公司	4	4
南京铱迅信息技术股份有限公司	2	2
东软	1	1
漏洞盒子	268	268
广西鑫瀚科技有限公司	11	11
清远职业技术学院	9	9
CNCERT 新疆分中心	4	4

CNCERT 湖北分中心	3	3
CNCERT 福建分中心	2	2
CNCERT 湖南分中心	2	2
CNCERT 江西分中心	2	2
CNCERT 宁夏分中心	2	2
CNCERT 山西分中心	1	1
CNCERT 吉林分中心	1	1
CNCERT 北京分中心	1	1
CNCERT 安徽分中心	1	1
个人	88	88
报送总计	1392	408
录入总计	109（去重）	408

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 109 个漏洞。其中应用程序漏洞 63 个，web 应用漏洞 18 个，网络设备漏洞 14 个，操作系统漏洞 13 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	63
web 应用漏洞	18
网络设备漏洞	14
操作系统漏洞	13
数据库漏洞	1

表 3 漏洞按影响类型统计表

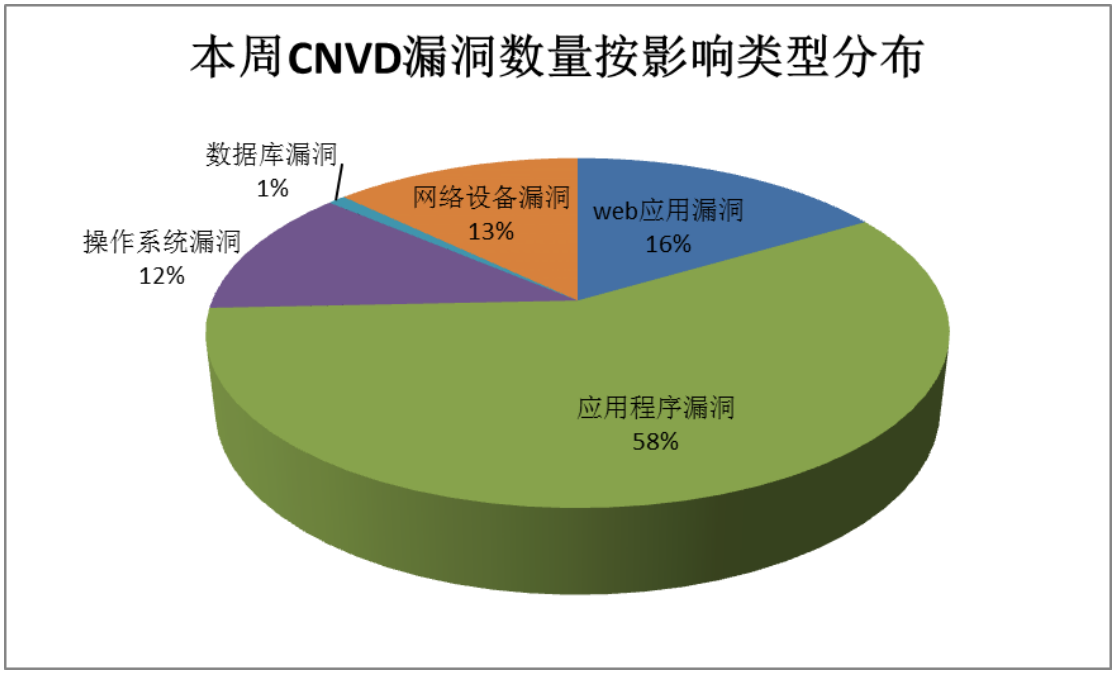

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Veritas Technologies、WordPress 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	12	11%
2	Veritas Technologies	10	9%
3	WordPress	8	7%
4	Foscam	7	6%
5	IBM	7	6%
6	General Electric	6	6%
7	Rapid7	6	6%
8	I-O DATA DEVICE, INC.	3	3%
9	OwnCloud	3	3%
10	其他	47	43%

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 1 个电信行业漏洞，13 个移动互联网行业漏洞，6 个工控系统行业漏洞（如下图所示）。其中，“Android Mediaserver 组件远程代码执行漏洞（CNVD-2017-02815、CNVD-2017-02817）、Android Mediaserver 组件远程代码执行漏洞、Andr

oid Qualcomm networking 驱动程序权限提升漏洞（CNVD-2017-02822）、Android Qualcomm networking 驱动程序权限提升漏洞、Android Qualcomm camera 驱动程序权限提升漏洞（CNVD-2017-02812、CNVD-2017-02814）、Android Qualcomm camera 驱动程序权限提升漏洞”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/

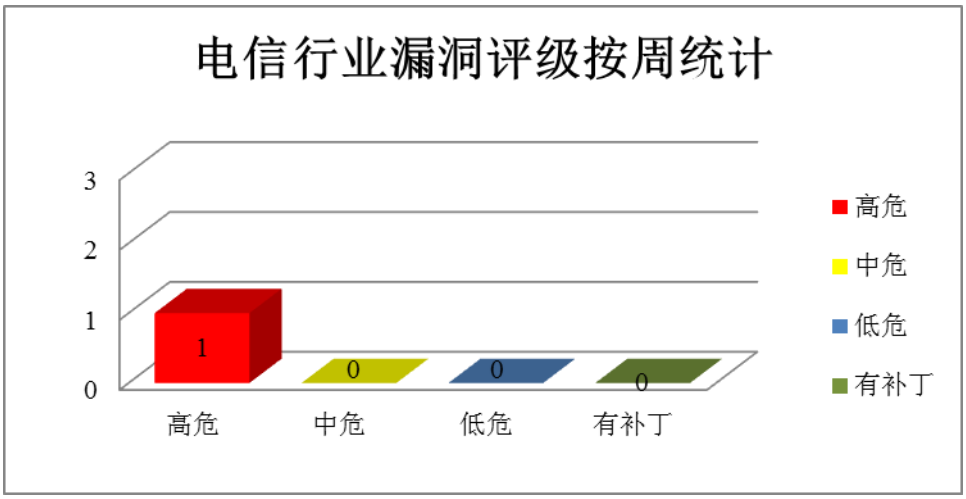

图 3 电信行业漏洞统计

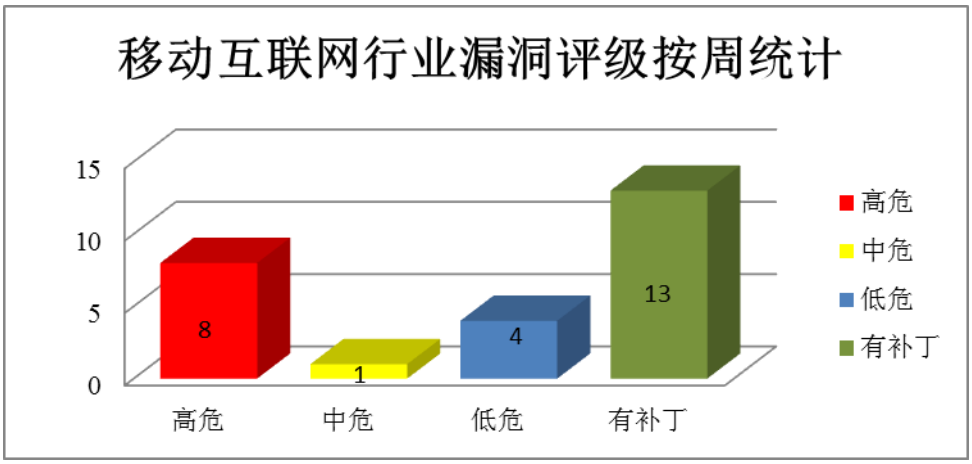

图 4 移动互联网行业漏洞统计

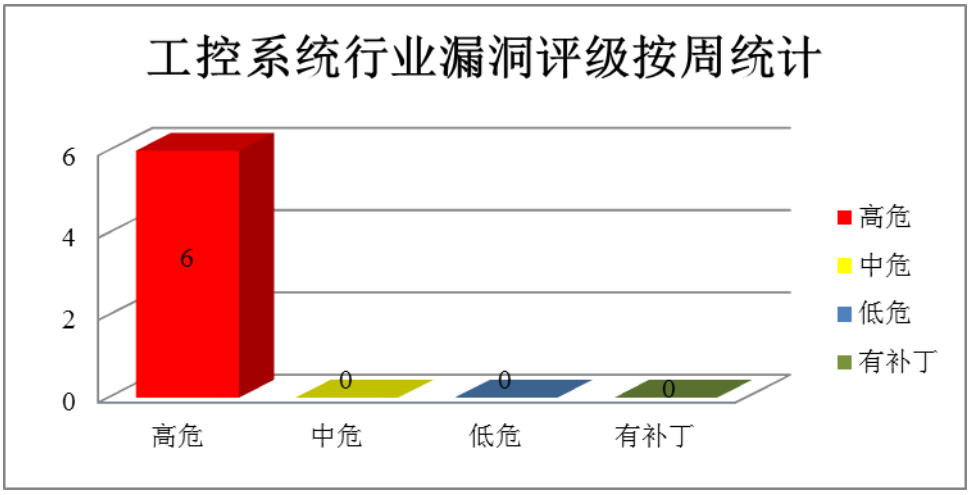

图 5 工控系统行业漏洞统计

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、Wireless IP Camera (P2P) WIFICAM 存在多个高危漏洞

Wireless IP Camera (P2P) WIFICAM 是一款无线 IP 摄像头。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制、获取敏感信息或执行任意代码等。

CNVD 收录的相关漏洞包括：Wireless IP Camera (P2P) WIFICAM ‘Cloud’功能设计缺陷漏洞、Wireless IP Camera (P2P) WIFICAMRSA 密钥和证书泄露漏洞、Wireless IP Camera (P2P) WIFICAM 存在后门漏洞、Wireless IP Camera (P2P) WIFICAM 未授权访问漏洞、Wireless IP Camera (P2P) WIFICAM 预授权信息和凭证泄漏漏洞、Wireless IP Camera (P2P) WIFICAM 预授权远程命令执行漏洞、Wireless IP Camera (P2P) WIFICAM 远程命令执行漏洞。其中，“Wireless IP Camera (P2P) WIFICAM ‘Cloud’功能设计缺陷漏洞、Wireless IP Camera (P2P) WIFICAM 未授权访问漏洞、Wireless IP Camera (P2P) WIFICAM 预授权信息和凭证泄漏漏洞、Wireless IP Camera (P2P) WIFICAM 存在后门漏洞”的综合评级为“高危”。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-2017-02778

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02773

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02751

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02777

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02774

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02776

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02775

2、SAP 云商务平台 HANA 系统存在多个高危漏洞

SAP 云商务平台 HANA 系统是一个基于内存计算技术的实时数据计算平台。本周，该产品被披露存在多个漏洞，其中会话固定和身份认证漏洞较为严重，攻击者可利用漏洞绕过身份验证和提升权限。

CNVD 收录的相关漏洞包括：SAP 云商务平台 HANA 系统会话固定漏洞、SAP 云商务平台 HANA 系统身份认证漏洞。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-2017-02802
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02799

3、Google 产品安全漏洞

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。Mediaserver 是其中的一个多媒体服务组件。Qualcomm networking Driver 是其中的一个网络连接库驱动程序。Qualcomm camera Driver 是使用在其中的一个美国高通（Qualcomm）公司开发的摄像头驱动程序。本周，上述产品被披露存在远程代码执行和权限提升漏洞，攻击者可利用漏洞提升权限和执行任意代码。

CNVD 收录的相关漏洞包括：Android Mediaserver 组件远程代码执行漏洞（CNVD-2017-02815、CNVD-2017-02817）、Android Mediaserver 组件远程代码执行漏洞、Android Qualcomm networking 驱动程序权限提升漏洞（CNVD-2017-02822）、Android Qualcomm networking 驱动程序权限提升漏洞、Android Qualcomm camera 驱动程序权限提升漏洞（CNVD-2017-02812、CNVD-2017-02814）、Android Qualcomm camera 驱动程序权限提升漏洞，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-2017-02815
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02817
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02813
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02822
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02821
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02812
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02514
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02511

4、Veritas 产品安全漏洞

Veritas Access 等都是美国 Veritas Technologies 公司的产品。Veritas Access 是一套用于非结构化数据的横向扩展 NAS 解决方案；Veritas NetBackup Appliance 是一款企业

级备份管理设备。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞发起拒绝服务攻击、执行任意代码或提升权限等。

CNVD 收录的相关漏洞包括：多款 Veritas 产品任意命令执行漏洞（CNVD-2017-02658）、多款 Veritas 产品本地命令执行漏洞、多款 Veritas 产品拒绝服务漏洞、多款 Veritas 产品硬编码凭证漏洞、多款 Veritas 产品目录遍历漏洞、多款 Veritas 产品任意命令执行漏洞、多款 Veritas 产品身份验证绕过漏洞、多款 Veritas 产品本地特权提升漏洞。其中，“多款 Veritas 产品硬编码凭证漏洞、多款 Veritas 产品目录遍历漏洞、多款 Veritas 产品任意命令执行漏洞、多款 Veritas 产品身份验证绕过漏洞”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-2017-02658
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02660
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02659
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02661
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02706
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02707
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02708
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02710

5、Dahua DHI-HCVR7216A-S3 中间人攻击漏洞

大华 DHI-HCVR7216A-S3 是中国大华（Dahua）公司的一款网络硬盘录像机产品。本周，大华被披露存在中间人攻击漏洞，攻击者可利用该漏洞创建拥有特权的新用户，执行中间人攻击，获取敏感信息。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-2017-02726

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-2017-02725	DBLTek GoIP 'dbladm'用户未授权访问漏洞	高	无
CNVD-2017-02729	多款 F5 BIG-IP 产品特权提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.f5.com/csp/article/K47284724
CNVD-2017-02737	WePresent WiPG-1500 后门漏洞	高	无
CNVD-2017-02736	Aruba AirWave Management Platform XML 外部实体注入漏	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接：

	洞		http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-001.txt
CNVD-2017-02744	多款 Intel 产品本地特权提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00070&languageid=en-fr
CNVD-2017-02749	7-ZIP32.DLL DLL 加载远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://blogs.technet.microsoft.com/srd/2010/08/23/more-information-about-the-dll-preloading-remote-attack-vector/
CNVD-2017-02798	大华科技摄像头产品非授权访问漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://us.dahuasecurity.com/en/us/Security-Bulletin_030617.php#none
CNVD-2017-02829	万户 ezOFFICE 协同办公系统 webservice 存在 SQL 注入漏洞	高	无
CNVD-2017-02830	麒麟堡垒机应用发布功能处存在文件上传漏洞	高	无

表 5 部分重要高危漏洞列表

小结：本周，Wireless IP Camera (P2P) WIFICAM 被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制、获取敏感信息或执行任意代码等。此外，SAP、Google、Veritas 等多款产品被披露存在多个漏洞，攻击者利用漏洞可泄露敏感信息、提升权限、执行任意代码或发起拒绝服务攻击等。另外，大华被披露存在中间人攻击漏洞，攻击者可利用该漏洞创建拥有特权的新用户，执行中间人攻击，获取敏感信息。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. 38 款 Android 设备预装恶意程序

CheckPoint 的专家们最近在 38 台 Android 设备中发现了严重的感染情况，这 38 台设备属于一家大型通讯公司和一家跨国科技企业。重点是这些恶意软件并不是用户主动安装的，而是在购买时就预装的。程序还会窃取设备数据、安装到系统，从而获得手机全部权限并常驻手机。更可怕的是，有 6 款恶意软件是利用了系统权限装到设备上的，也就是说除非刷机，用户无法移除软件。建议大家从正规渠道购买手机，这样才不致如上面这些手机一样，在非正规供货渠道预装恶意程序。

参考链接：http://www.freebuf.com/news/129267.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：010-82990999