国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 04 月 24 日-2017 年 04 月 30 日 **2017 年第 18 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 394 个，其中高危漏洞 131 个、中危漏洞 235 个、低危漏洞 28 个。漏洞平均分值为 6.05。本周收录的漏洞中，涉及 0day 漏洞 61 个（占 15%），其中互联网上出现“部分厂商设备 SNMP 协议社区字符串认证权限绕过漏洞、Intellinet NFC-30ir IP Camera 安全绕过漏洞”零日代码攻击漏洞，同时本周出现了多个应用广泛的软硬件产品高危漏洞。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 751 个，与上周（661 个）环比增长 14%。

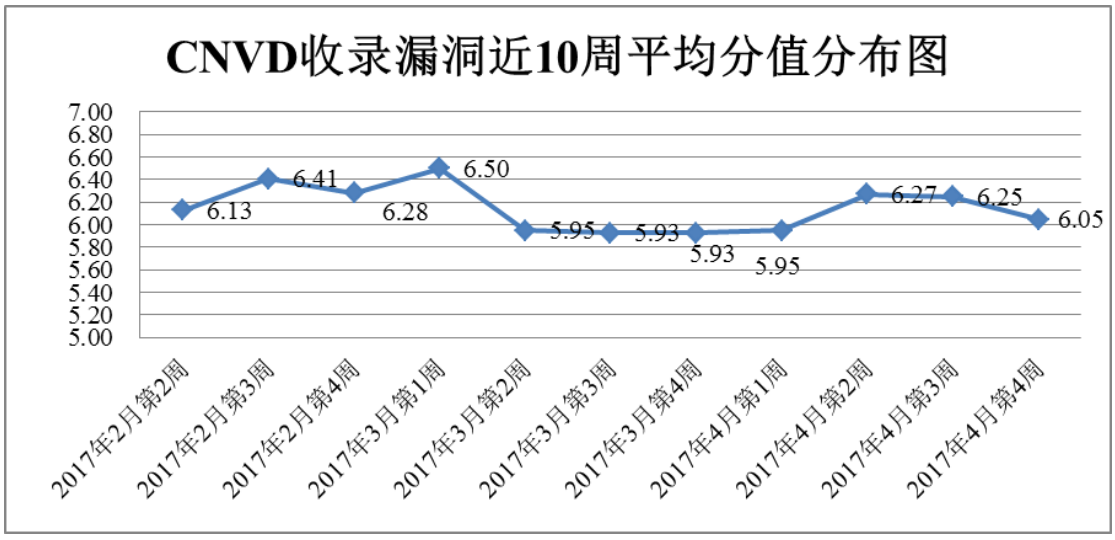

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 394 个漏洞。报送情况如表 1 所示。其中，启明星辰、安天实验室、东软、天融信、绿盟科技等单位报送数量较多。安徽新华博信息技术股份有限公司、山石网科通信技术有限

公司、江苏君立华域信息安全技术有限公司、广州万方计算机科技有限公司、广州市网迅信息技术有限公司、中新网络信息安全股份有限公司、清远职业技术学院、山东安云信息技术有限公司、江西安服信息产业有限公司、北京安码科技有限公司、广西网信信息安全等级保护测评有限公司 及其他个人白帽子向 CNVD 提交了 751 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
360 网神	343	343
启明星辰	405	2
安天实验室	188	0
东软	121	0
天融信	100	1
绿盟科技	86	0
华为技术有限公司	70	2
H3C	55	0
中国电信集团系统集成有限责任公司	54	0
杭州安恒信息技术有限公司	48	0
厦门服云信息科技有限公司	24	1
恒安嘉新	10	0
广西鑫瀚科技有限公司	9	9
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
北京知道创宇信息技术有限公司	2	2
漏洞盒子	207	207

安徽新华博信息技术股份有限公司	22	22
山石网科通信技术有限公司	11	11
江苏君立华域信息安全技术有限公司	6	6
广州万方计算机科技有限公司	5	5
广州市网迅信息技术有限公司	4	4
中新网络信息安全股份有限公司	2	2
清远职业技术学院	2	2
山东安云信息技术有限公司	1	1
江西安服信息产业有限公司	1	1
北京安码科技有限公司	1	1
广西网信信息安全等级保护测评有限公司	1	1
CNCERT 重庆分中心	9	9
CNCERT 福建分中心	8	8
CNCERT 甘肃分中心	6	6
CNCERT 河北分中心	4	4
CNCERT 新疆分中心	4	4
CNCERT 湖南分中心	3	3
CNCERT 江西分中心	2	2
CNCERT 上海分中心	2	2
CNCERT 广东分中心	1	1
CNCERT 北京分中心	1	1
个人	82	82
报送总计	1911	751

录入总计	394（去重）	751

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 394 个漏洞。其中应用程序漏洞 233 个，操作系统漏洞 69 个，web 应用漏洞 49 个，网络设备漏洞 40 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	233
操作系统漏洞	69
web 应用漏洞	49
网络设备漏洞	40
安全产品漏洞	3

表 2 漏洞按影响类型统计表

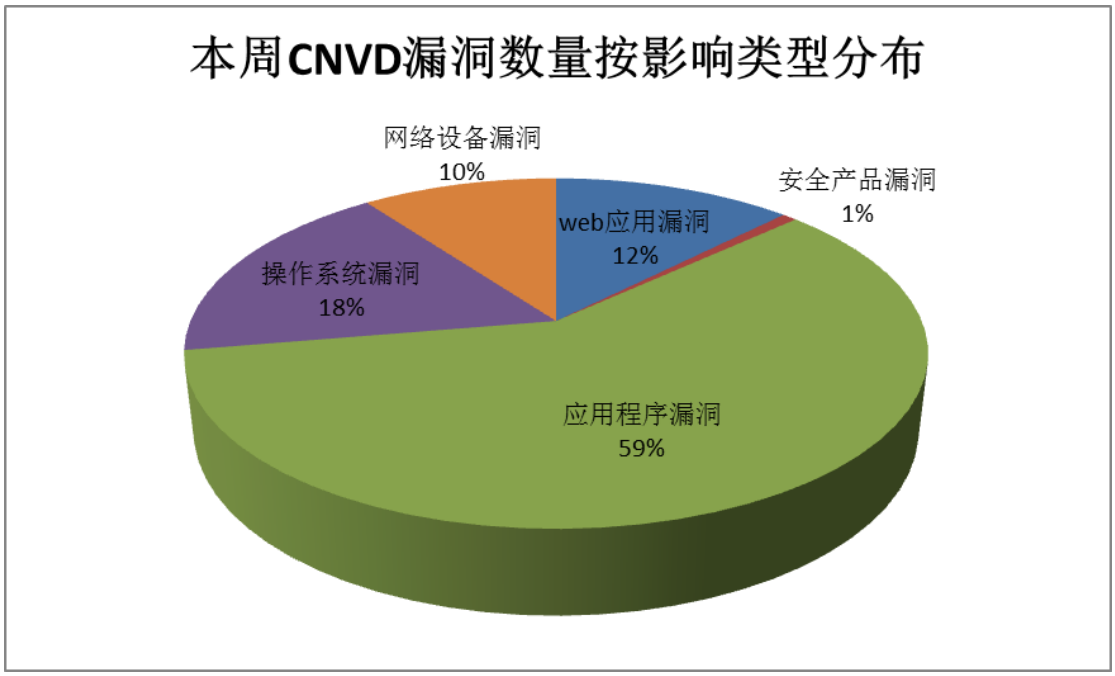

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、Google、Cisco 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	Apple	34	9%
2	Google	13	3%
3	Cisco	13	3%
4	Microsoft	13	3%

5	Silicon Graphics, Inc.	12	3%
6	Linux	10	3%
7	IBM	9	2%
8	elfintils	7	2%
9	Adobe	6	2%
10	其他	277	70%

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 15 个电信行业漏洞，32 个移动互联网行业漏洞，7 个工控系统行业漏洞（如下图所示）。其中，“多款 Cisco 产品本地命令执行漏洞、多款 Jensen of Scandinavia Air:Link 命令执行漏洞、Bluecoat ASG 6.6/CAS OS 命令注入漏洞漏洞、Google Android NFC 权限提升漏洞、Google Android libskia 拒绝服务漏洞、Google Android Mediaserver 代码执行漏洞、Google Android Qualcomm Audio Driver 权限提升漏洞、Google Android Qualcomm Kyro L2 driver 权限提升漏洞”等的综合评级为“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/

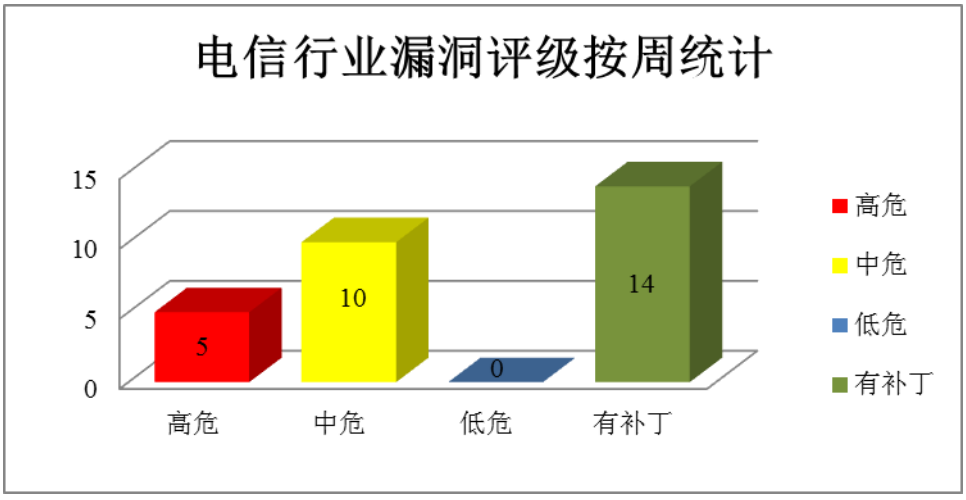

图 3 电信行业漏洞统计

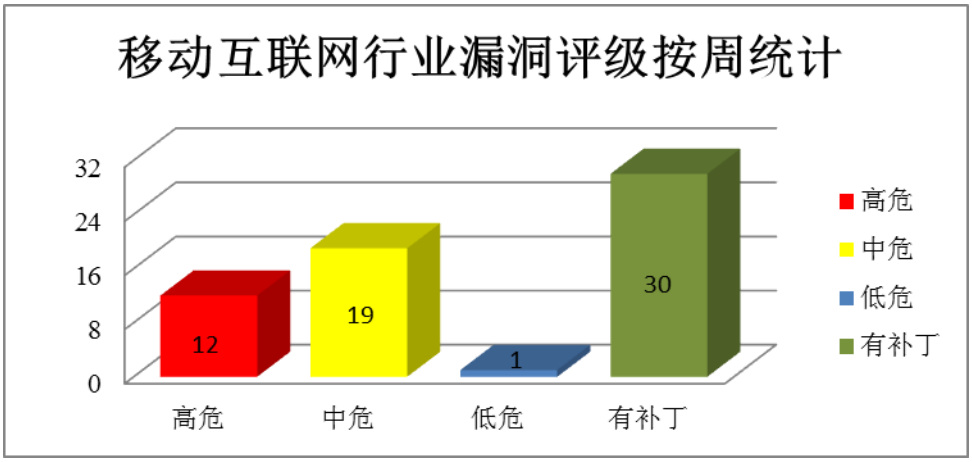

图 4 移动互联网行业漏洞统计

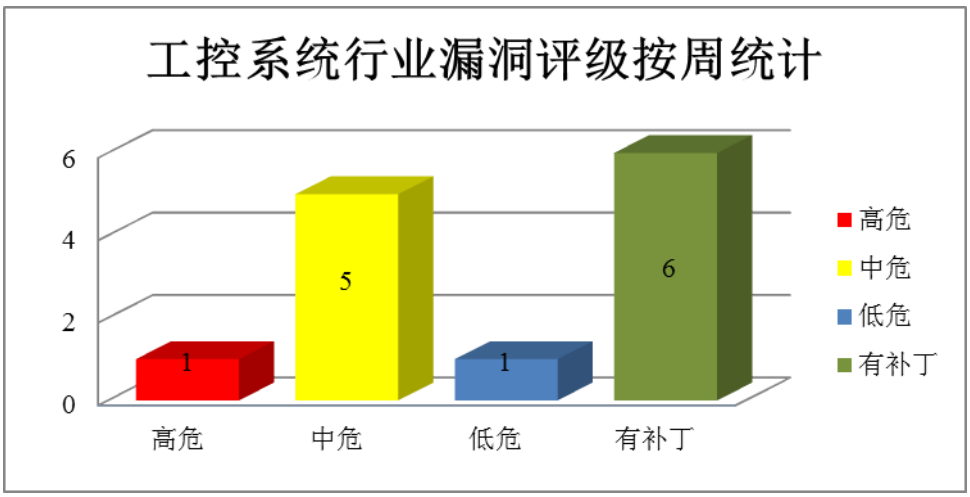

图 5 工控系统行业漏洞统计

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、部分厂商设备存在 SNMP 协议社区字符串认证权限绕过漏洞

SNMP 是基于 TCP/IP 协议族的网络管理标准，是一种在 IP 网络中管理网络节点的标准协议。本周，部分厂商设备被披露存在 SNMP 协议社区字符串认证权限绕过漏洞，攻击者可利用漏洞绕过安全限制，获取权限。

CNVD 收录的相关漏洞包括：部分厂商设备存在 SNMP 协议社区字符串认证权限绕过漏洞。该漏洞的综合评级为“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-2017-05535

2、Jenkins 存在 Java 反序列化等多个漏洞

Jenkins 是一个开源软件项目，基于 Java 开发的一种持续集成工具。Jenkins CLI 工具允许用户通过命令行来操作 Jenkins。本周，该产品被披露存在多个漏洞，攻击者可利

用漏洞执行任意代码、冒充 Jenkins 用户或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Jenkins Java 反序列化远程执行代码漏洞、Jenkins 存在多个跨站请求伪造漏洞、Jenkins 拒绝服务漏洞、Jenkins 用户登录信息泄露漏洞。其中，“Jenkins 拒绝服务漏洞、Jenkins Java 反序列化远程执行代码漏洞”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-2017-05551

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05570

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05571

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05572

3、zabbix 存在数据库写入和代码执行漏洞

Zabbix 是一个基于 WEB 界面的提供分布式系统监视以及网络监视功能的企业级的开源解决方案本周，该产品被披露存在数据库写入和代码执行漏洞，攻击者可利用漏洞执行操作系统指令，取得网站服务器控制权限。

CNVD 收录的相关漏洞包括：Zabbix 存在远程代码执行和数据库写入漏洞。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-2017-05550

4、Apple 产品安全漏洞

Apple macOS 是美国苹果（Apple）公司为 Mac 计算机所开发的一套专用操作系统。Bluetooth 是一个蓝牙组件。IOFireWireAVC 是一个 IO 视频传输组件。Intel Graphics Driver 是一个显卡驱动。MCX Client 是一个管理客户端。 IOATAFamily 是一个 ATI 芯片驱动组件。Kernel 是一个内核组件。本周，上述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、执行任意代码和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Apple macOS Bluetooth 权限提升漏洞（CNVD-2017-05624）、Apple macOS Bluetooth 权限提升漏洞、Apple macOS IOFireWireAVC 权限提升漏洞、Apple macOS Intel Graphics Driver 任意代码执行漏洞、Apple macOS Sierra Bluetooth 权限提升漏洞、Apple macOS Sierra MCX Client 安全绕过漏洞、Apple mac OS Sierra IOATAFamily 拒绝服务漏洞、Apple macOS Sierra Kernel 任意代码执行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-2017-05624

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05621

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05620

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05619

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05601

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05143

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05141

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05139

5、PHPCMS WAP 模块任意文件下载漏洞

PHPCMS 是一款网站管理软件。本周，PHPCMS 被披露存在任意文件下载漏洞，攻击者利用该漏洞无需登录即可访问。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-2017-05511

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-2017-05213	OpenSSH xauth 输入验证漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.openssh.com/txt/x11fwd.adv
CNVD-2017-05236	Bluecoat ASG 6.6/CAS OS 命令注入漏洞漏洞	高	用户可联系供应商获得补丁信息：https://bto.bluecoat.com/security-advisory/sa138
CNVD-2017-05278	Artifex Software MuJS 缓冲区溢出漏洞（CNVD-2017-05278）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://mujs.com/
CNVD-2017-05302	多款 Jensen of Scandinavia Air:Link 命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.jensenofscandinavia.com/
CNVD-2017-05441	SAP NetWeaver 缓冲区溢出漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.sap.com/index.html
CNVD-2017-05476	Botan 拒绝服务漏洞（CNVD-2017-05476）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://botan.randombit.net/security.html#id3
CNVD-2017-05509	MyBB MyCode 模块跨站脚本漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://mybb.com/
CNVD-2017-05510	Ansible 不完全修复任意命令执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://www.ansible.com/
CNVD-201	Zyxel WRE6505 DNS 劫持漏洞	高	厂商已发布漏洞修复程序，请及时关

7-05673			注更新：ftp://ftp2.zyxel.com/WRE6505/firmware/
CNVD-2017-05675	Apache Batik XXE 信息泄露漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://xmlgraphics.apache.org/security.html

表 4 部分重要高危漏洞列表

小结：本周，部分厂商设备被披露存在 SNMP 协议社区字符串认证权限绕过漏洞。攻击者可利用漏洞绕过安全限制，获取权限此外，Jenkins、zabbix、Apple 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、绕过安全限制、提升权限或发起拒绝服务攻击等。另外，PHPCMS 被披露存在任意文件下载漏洞，攻击者利用该漏洞无需登录即可访问。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. 所有版本的 IE 浏览器都存在的一个 0day 漏洞

通过研究发现，如果你打开一个.eml 文件，那么 IE 浏览器将会执行 mime 嗅探，如果在响应信息中识别到了 HTML/JS 文件，浏览器将会执行这些代码。EML 代表“Microsoft Outlook Express mail message”，也就是微软 Outlook 的邮件信息，这种格式允许我们将邮件信息保存在文件中。你可以将该文件保存在 Web 服务器中，并通过 IE 浏览器来访问它。你将会看到浏览器呈现出正确的内容。这个漏洞将会影响所有版本的 IE 浏览器（已在 Win7、Win8.1 和 Win10 上进行了测试）。最简单的解决方案就是在样本文件中添加 header（‘X-Frame-Options:DENY’）就可以防止这漏洞被利用了。

参考链接：http://www.freebuf.com/articles/web/132963.html

2. SNMP 协议漏洞影响多种网络设备

据来自南美的两位安全研究者发现，SNMP（简单网络管理协议）的 v1 和 v2 版本协议存在授权认证和访问控制绕过漏洞，至少有 78 种型号的网络接入和 IoT 设备受此漏洞影响，攻击者可以利用该漏洞远程获得相关设备的读写权限，进而控制设备。这一漏洞被发现者命名为 Stringbleed，受影响的设备产品类型涉及路由器、VoIP 网关、IoT 设备和其他拨号网关等。

参考链接：http://www.freebuf.com/vuls/133517.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