国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 02 月 06 日-2017 年 02 月 12 日 **2017 年第 7 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**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 242 个，其中高危漏洞 84 个、中危漏洞 142 个、低危漏洞 16 个。漏洞平均分值为 6.05。本周收录的漏洞中，涉及 0day 漏洞 41 个（占 17%）。其中互联网上出现“NETWAVE IP Camera 密码泄露漏洞、BoZoN 远程代码执行漏洞”等零日代码攻击漏洞，请使用相关产品的用户注意加强防范。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 773 个，与上周（199 个）环比增长 288%。

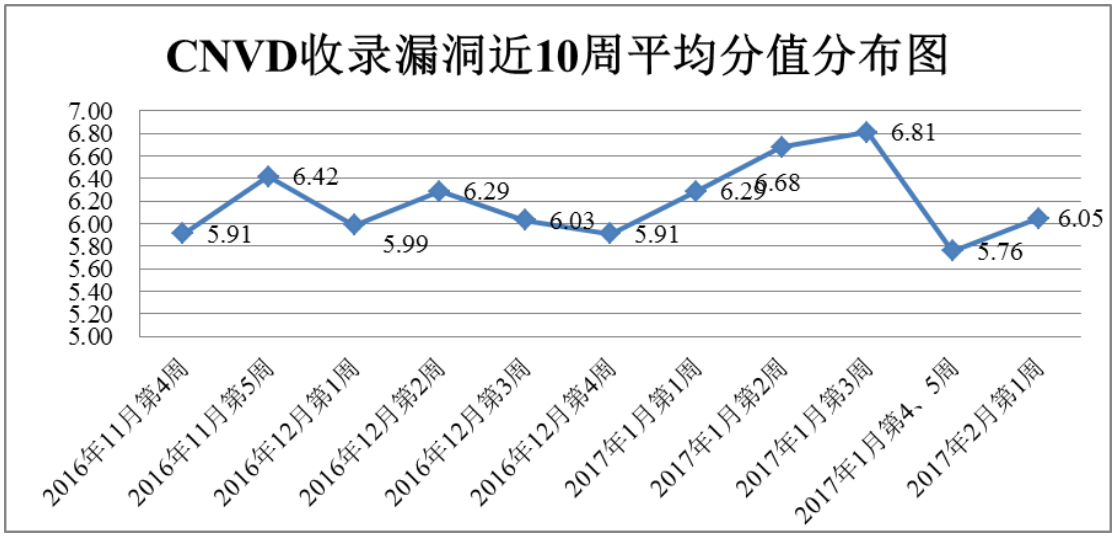

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 15 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 242 个漏洞。报送情况如表 1 所示。其中，蓝盾信息安全技术股份有限公司、启明星辰、安天实验室、华为技术有限公司等单位报送数量较多。360 网神、漏洞盒子、广西鑫瀚科技有限公司、北京安码科技有限公司、广州圣辉信息技术有限公司及其他个人白帽子向 C

NVD 提交了 773 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	555	555
蓝盾信息安全技术有限公司	233	0
启明星辰	187	3
安天实验室	147	0
华为技术有限公司	96	0
天融信	93	1
绿盟科技	60	0
恒安嘉新	9	0
中国电信集团系统集成有限责任公司	47	0
H3C	45	0
杭州安恒信息技术有限公司	18	0
西安四叶草信息技术有限公司	7	7
安全狗	3	0
知道创宇	2	0
北京数字观星科技有限公司	1	0
南京铱迅信息技术股份有限公司	1	1
漏洞盒子	125	125
广西鑫瀚科技有限公司	4	4
北京安码科技有限公司	4	4
广州圣辉信息技术有限公司	2	2
CNCERT 陕西分中心	4	4

CNCERT 浙江分中心	3	3
CNCERT 宁夏分中心	3	3
CNCERT 广东分中心	2	2
CNCERT 湖南分中心	2	2
CNCERT 甘肃分中心	2	2
CNCERT 海南分中心	1	1
个人	54	54
报送总计	1710	773
录入总计	242（去重）	773

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 242 个漏洞。其中应用程序漏洞 143 个，web 应用漏洞 34 个，网络设备漏洞 33 个，操作系统漏洞 16 个，数据库漏洞 14 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	143
web 应用漏洞	34
网络设备漏洞	33
操作系统漏洞	16
数据库漏洞	14
安全产品漏洞	2

表 2 漏洞按影响类型统计表

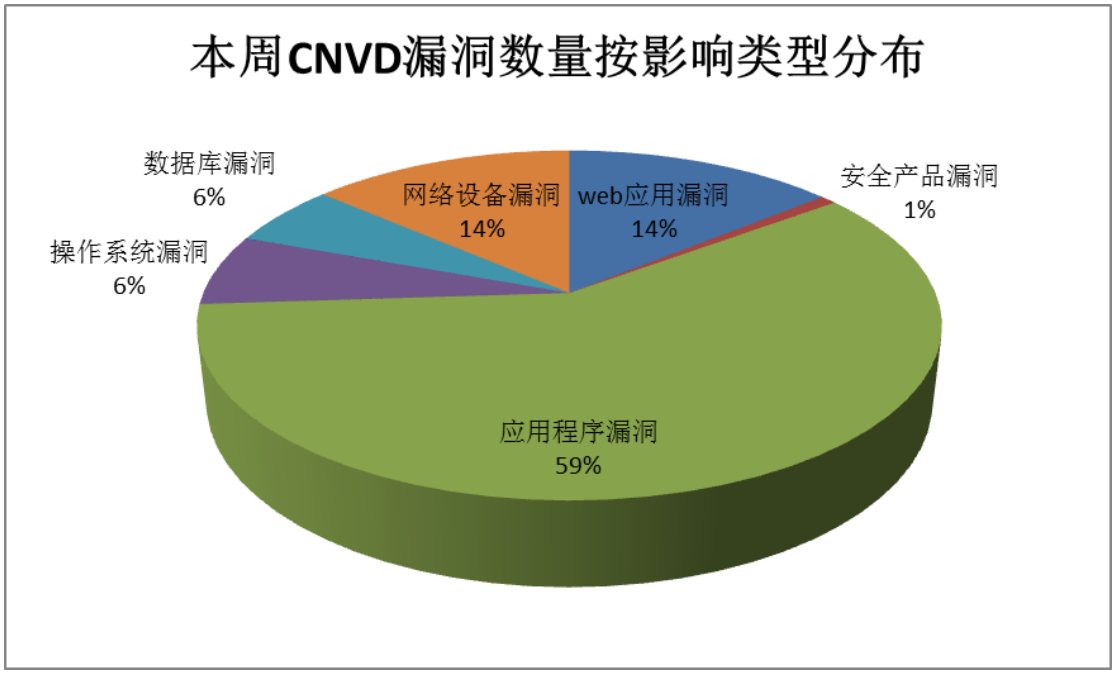

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Cisco、EMC 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	Oracle	37	15%
2	Cisco	17	7%
3	EMC	17	7%
4	IBM	12	5%
5	Tcpdump	10	4%
6	Jasper	7	3%
7	ImageMagick	6	3%
8	PHP	6	3%
9	D-Link	6	3%
10	其他	124	50%

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 26 个电信行业漏洞，13 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图所示）。其中，“NETGEAR WNR2000v5 router hidden_lang_avi 缓冲区溢出漏洞、D-Link DWR-932B SHELL 命令执行漏洞、D-Link DWR-932B 命令注

入漏洞、Cisco ASR 1000 Series Routers 拒绝服务漏洞、Oracle MySQL Server 存在未明漏洞（CNVD-2017-00992）、Apple iOS/tvOS/watchOS 任意代码执行漏洞、Apple iTunes/iCloud/Safari/iOS 存在多个内存破坏漏洞、Samsung 远程内存破坏漏洞”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/

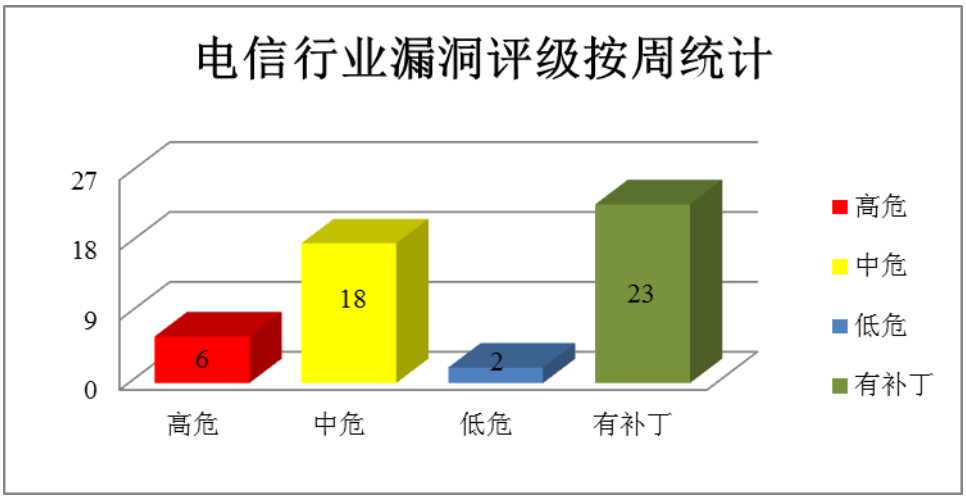

图 3 电信行业漏洞统计

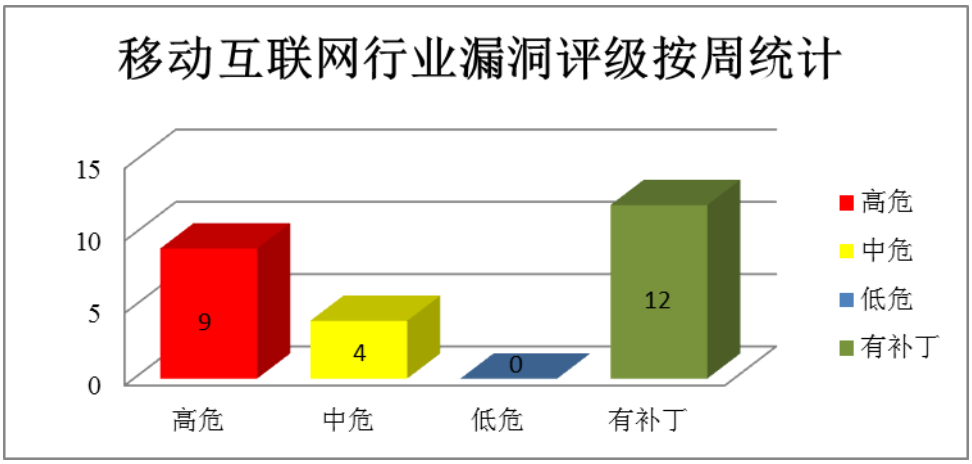

图 4 移动互联网行业漏洞统计

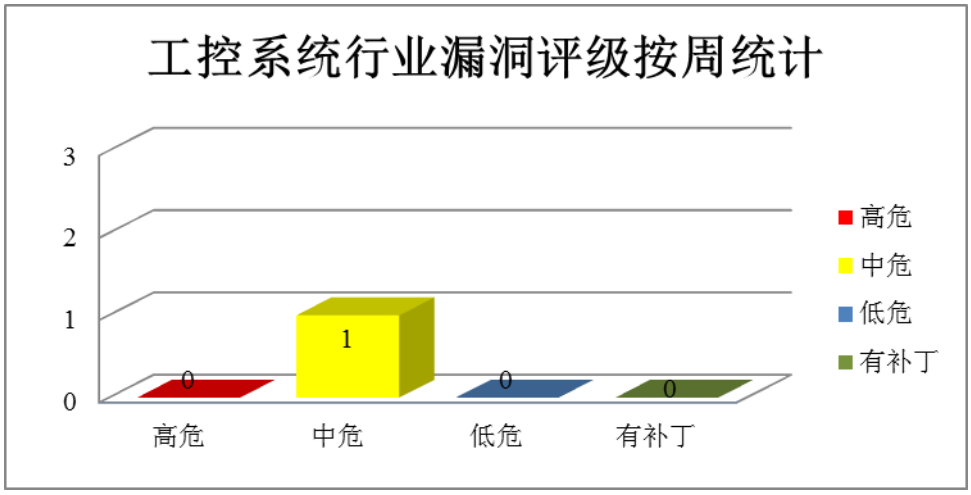

图 5 工控系统行业漏洞统计

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、F5 BIG-IP 产品安全漏洞

F5 BIG-IP 是美国 F5 公司的一款集成了网络流量管理、应用程序安全管理、负载均衡等功能的多合一网络设备。本周，该产品被披露存在 TicketBleed 漏洞，攻击者可利用漏洞获取密钥或敏感数据。

CNVD 收录的相关漏洞包括：F5 BIG-IP 设备存在 TicketBleed 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-2017-01171

2、Node.js 存在产品安全漏洞

Node.js 是一个基于 Chrome JavaScript 运行时建立的平台。本周，该产品被披露存在反序列化远程代码执行漏洞，攻击者可利用漏洞执行反序列化远程代码操作，以获取主机权限。

CNVD 收录的相关漏洞包括：Node.js 存在反序列化远程代码执行漏洞，该漏洞的综合评级为“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-2017-01206

3、IBM 产品安全漏洞

IBM AppScan Enterprise Edition 是一款安全漏洞扫描解决方案。IBM Security Key Lifecycle Manager、IBM Tivoli Key Lifecycle Manager 都是美国 IBM 公司的一套密钥生命周期管理软件。IBM Kenexa LMS on Cloud 是一套企业级社交学习管理系统。本周，上述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

或上传任意文件等。

CNVD 收录的相关漏洞包括：IBM AppScan Enterprise Edition 任意代码执行漏洞、IBM Jazz for Service Management 信息泄露漏洞、IBM Kenexa LMS on Cloud 任意文件上传漏洞（CNVD-2017-01017）、IBM Security Key Lifecycle Manager 身份验证绕过漏洞、IBM Security Key Lifecycle Manager 跨站请求伪造漏洞、IBM Security Key Lifecycle Manager 信息泄露漏洞（CNVD-2017-01134、CNVD-2017-01135）、IBM Tivoli Key Lifecycle Manager 未授权访问漏洞。其中“IBM AppScan Enterprise Edition 任意代码执行漏洞、IBM Jazz for Service Management 信息泄露漏洞、IBM Kenexa LMS on Cloud 任意文件上传漏洞（CNVD-2017-01017）、IBM Security Key Lifecycle Manager 身份验证绕过漏洞”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-2017-01197

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01222

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01017

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01137

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01136

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01134

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01135

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01198

4、EMC 产品安全漏洞

EMC Network Configuration Manager 是美国易安信（EMC）公司的一款智能网络配置管理器。EMC Isilon InsightIQ 提供了性能监控和报告工具。EMC Data Protection Advisor 是一款统一的数据保护管理解决方案。EMC Documentum eRoom 是一套基于 Web 的共享工作平台，EMC Isilon OneFS 是一套支持 EMC Isilon（横向扩展存储系统）的分布式文件系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞远程执行任意代码、提升权限、更改密码或绕过身份验证等。

CNVD 收录的相关漏洞包括：EMC Isilon InsightIQ 认证绕过漏洞、EMC Data Protection Advisor 目录遍历漏洞、EMC Network Configuration Manager 身份验证漏洞、EMC Network Configuration Manager 远程代码执行漏洞、EMC Documentum eRoom 管理密码更改认证绕过漏洞、EMC Isilon OneFS 权限提升漏洞（CNVD-2017-01155）、EMC RecoverPoint 和 EMC RecoverPoint for Virtual Machines 命令注入漏洞、EMC Isilon OneFS 本地 LDAP 注入漏洞。除“EMC Data Protection Advisor 目录遍历漏洞”外，其余漏洞的综合评级为“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-2017-01150

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01153

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01151

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01152

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01161

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01155

http://www.cnvd.org.cn/flaw/show/CNVD-2017-01146

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00981

5、HP Printers Wi-Fi 未授权访问漏洞

HP Printers Wi-Fi 是美国惠普（HP）公司的一款 WiFi 直连打印机。本周，HP 被披露存在未授权访问漏洞。攻击者可利用漏洞获取打印机网络信息，修改防火墙配置等。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-2017-01038

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-2017-01234	Tcpdump OTV 析器缓冲区溢出漏洞	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.tcpdump.org
CNVD-2017-01233	Tcpdump ISAKMP 析器缓冲区溢出漏洞	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.tcpdump.org
CNVD-2017-01232	Tcpdump IPv6 析器缓冲区溢出漏洞	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.tcpdump.org
CNVD-2017-01231	Tcpdump BOOTP 解析器缓冲区溢出漏洞	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.tcpdump.org
CNVD-2017-01227	WordPress WP_Query SQL 注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://codex.wordpress.org/Version_4.7.2
CNVD-2017-01236	Tcpdump Q.933 解析器缓冲区溢出漏洞	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.tcpdump.org
CNVD-2017-01235	Tcpdump 多个解析器缓冲区溢出漏洞	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.tcpdump.org
CNVD-201	Adobe Acrobat Reader 缓冲区溢	高	目前厂商已经发布了升级补丁以修

7-01245	出漏洞（CNVD-2017-01245）		复此安全问题，补丁获取链接：https://helpx.adobe.com/security/products/acrobat/apsb17-01.html
CNVD-2017-01242	FFmpeg 整数溢出漏洞（CNVD-2017-01242）	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：https://www.ffmpeg.org/security.html
CNVD-2017-01240	Tcpdump ISO CLNS 解析器缓冲区溢出漏洞	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.tcpdump.org

表 4 部分重要高危漏洞列表

小结：本周，F5 BIG-IP 被披露存在 TicketBleed 漏洞，攻击者可利用漏洞获取密钥或敏感数据。此外，Node.js、IBM、EMCl 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、泄露敏感信息或绕过身份验证等。另外，HP 被披露存在未授权访问漏洞。攻击者可利用漏洞获取打印机网络信息，修改防火墙配置等。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. 15 万台打印机被黑，打印出了一堆奇怪的东西

近日，国外有一个自称“stackoverflowin”的黑客侵入了超过 15 万台打印机。被入侵的这些打印机全部都打印出了这名黑客留下的警告信息。受到影响的品牌包括 Afico，Brother，佳能，爱普生，惠普，利盟，柯尼卡美能达，Oki 和三星。攻击者可借助这个漏洞注入 PostScript，完成强制远程打印工作。好在这是一次善意的“攻击”，假如这些打印机漏洞被恶意地利用，很有可能就形成一个类似于 Mirai 的僵尸网络，后果不堪设想。

参考链接：http://www.freebuf.com/news/126063.html

2. Anonymous 攻陷暗网服务提供商 Freedom Hosting II

Freedom Hosting II（以下简称 FH II）是现今最大的暗网服务提供商之一。据 Mascherari.press 的安全专家 Sarah Jamie Lewis 估算，FH II 约为 15%-20%的暗网网站提供服务。这类网站的域名通常为.onion 且可以通过洋葱浏览器（Tor Browser）访问。攻击者可通过开设新网站或登录已存在网站，修改配置文件并重设密码后获得 root 权限。

参考链接：http://www.freebuf.com/news/126335.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