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 06 日-2017 年 03 月 12 日 **2017 年第 11 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 193 个，其中高危漏洞 82 个、中危漏洞 100 个、低危漏洞 11 个。漏洞平均分值为 6.5。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“NETGEAR DGN2200 任意命令执行漏洞、Joomla com_news 组件'id'参数 SQL 注入漏洞”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超过 1800 个(不完全统计)，与上周（347 个）相比有数倍增长，主要是由于 Apache Struts 2 S2-045 漏洞利用代码的出现，导致大量网站服务器面临攻击风险。

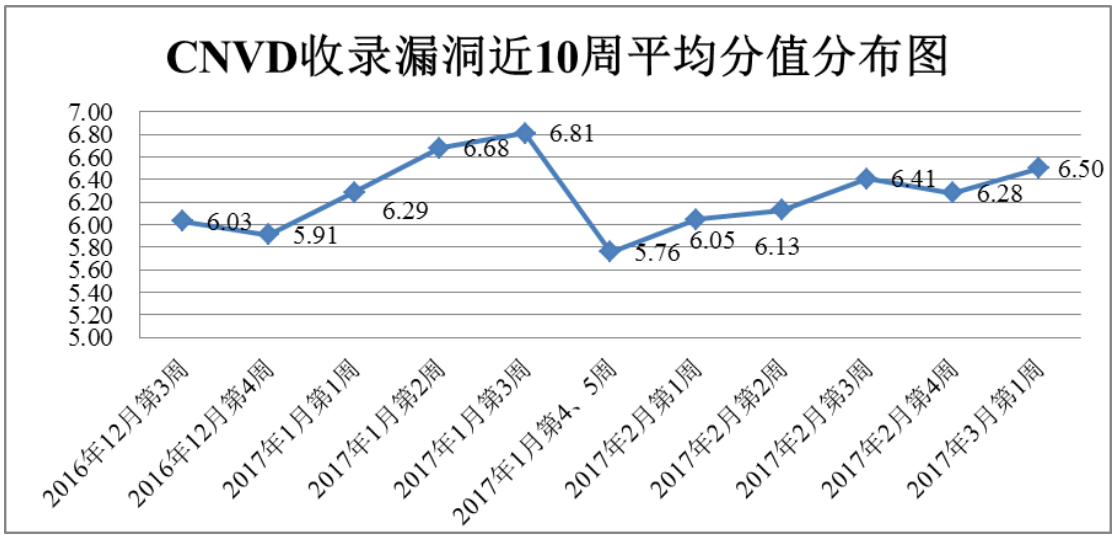

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 14 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 193 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、启明星辰等单位报送数量较多。漏洞盒子、中新网络信息安

全股份有限公司及其他个人白帽子向 CNVD 提交了 724 个以事件型漏洞为主的原创漏洞（暂不包含 CNVD 前台白帽子和 CNVD 成员单位提交 S2-045 漏洞案例数据），其中漏洞及时与 CNVD 共享了涉及党政机关、高校等单位的 S2-045 漏洞风险信息。

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	153	6
安天实验室	118	0
天融信	102	1
华为技术有限公司	90	0
启明星辰	87	5
恒安嘉新	69	0
H3C	47	0
安全狗	37	2
绿盟科技	31	0
中国电信集团系统集成有限责任公司	25	0
杭州安恒信息技术有限公司	20	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	7	7
南京铱迅信息技术股份有限公司	1	1
漏洞盒子	647	647
中新网络信息安全股份有限公司	1	1
CNCERT 江西分中心	8	8
CNCERT 重庆分中心	7	7
CNCERT 上海分中心	1	1
CNCERT 宁夏分中心	1	1

CNCERT 福建分中心	1	1
个人	36	36
报送总计	1494	724
录入总计	193（去重）	724

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 200 个漏洞。其中应用程序漏洞 92 个，web 应用漏洞 58 个，操作系统漏洞 21 个，网络设备漏洞 19 个，数据库漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	92
web 应用漏洞	58
操作系统漏洞	21
网络设备漏洞	19
数据库漏洞	3

表 3 漏洞按影响类型统计表

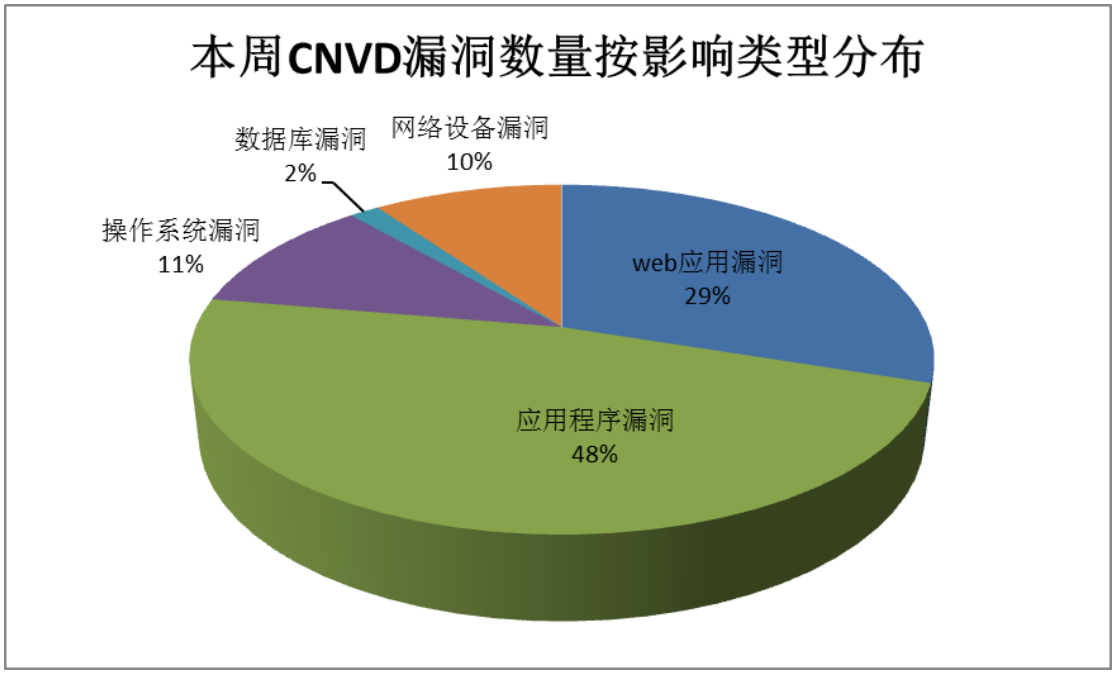

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、IBM、Joomla 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	WordPress	14	7%

2	IBM	13	7%
3	Joomla	11	6%
4	Apple	10	5%
5	ytnef	9	4%
6	Linux	8	4%
7	Iceni Technology	6	3%
8	北京联杰海天科技有限公司	5	2%
9	D-Link	4	2%
10	其他	113	60%

表 4 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 17 个电信行业漏洞，7 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，“多款 D-Link 产品栈缓冲区溢出漏洞、NETGEAR DGN2200 远程执行代码漏洞、Red Lion Controls Sixnet-Managed Industrial Switches 和 Stride-Managed Ethernet Switches 硬编码加密密钥漏洞、NetCommWireless Wireless Router 远程命令注入漏洞、Apple iOS WebSheet 组件沙盒绕过漏洞”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/

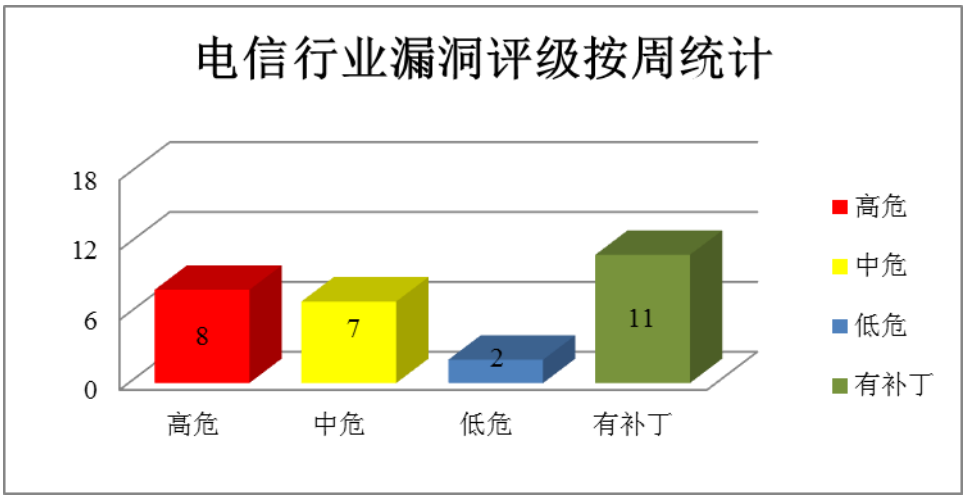

图 3 电信行业漏洞统计

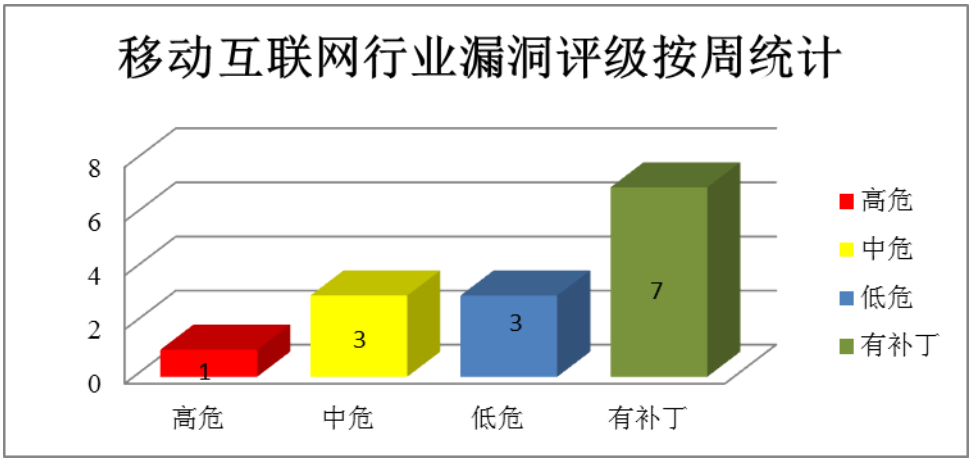

图 4 移动互联网行业漏洞统计

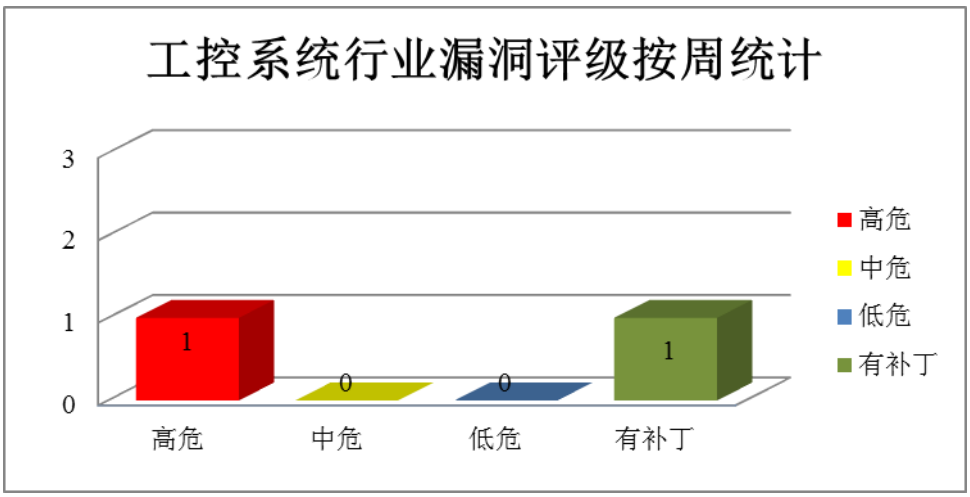

图 5 工控系统行业漏洞统计

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、Apache Struts2 存在 S2-045 远程代码执行漏洞

Apache Struts 是一款用于创建企业级 Java Web 应用的开源框架。本周，该产品被披露存在 S2-045 远程代码执行漏洞，攻击者可利用漏洞直接取得网站服务器控制权。

CNVD 收录的相关漏洞包括：Apache Struts2 存在 S2-045 远程代码执行漏洞。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-2017-02474

2、Apple 产品安全漏洞

Apple macOS Sierra 是美国苹果公司为 Mac 计算机所开发的一套专用操作系统。Apple iOS 是一套为移动设备所开发的操作系统。watchOS 是一套智能手表操作系统。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息、进行跨站脚本攻

击或执行任意代码等。

CNVD 收录的相关漏洞包括：Apple macOS Sierra libxpc 组件沙盒绕过漏洞、Apple iOS WebKit 组件跨站脚本漏洞、Apple iOS/macOS 拒绝服务漏洞、Apple iOS Clipboard 组件信息泄露漏洞、Apple iOS WebSheet 组件沙盒绕过漏洞、Apple macOS 本地信息泄露漏洞、Apple macOS 任意代码执行漏洞（CNVD-2017-02450、CNVD-2017-02451）。其中，“Apple iOS WebSheet 组件沙盒绕过漏洞、Apple macOS 任意代码执行漏洞（CNVD-2017-02450）”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-2017-02507
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02426
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02438
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02440
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02439
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02442
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02450
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02451

3、IBM 产品安全漏洞

IBM Tivoli System Automation for Multiplatforms 是美国 IBM 公司的一套集群解决方案。IBM Content Navigator 是一款 Web 客户机，IBM WebSphere MQ 是一款消息传递中间件产品。IBM PowerKVM 是一套开放式虚拟化解决方案。IBM Tivoli Storage Manager Server 是一套存储管理软件解决方案。IBM Jazz for Service Management 在整合服务管理和一些关键领域的第三方产品提供了增强的解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞进行跨站脚本攻击、提升本地权限、执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM Tivoli System Automation for Multiplatforms 本地权限提升漏洞、IBM Content Navigator 跨站脚本漏洞（CNVD-2017-02624）、IBM WebSphere MQ 拒绝服务漏洞（CNVD-2017-02626、CNVD-2017-02480）、IBM PowerKVM 命令执行漏洞、IBM Tivoli Storage Manager Server 缓冲区溢出漏洞、IBM WebSphere MQ 数据转换拒绝服务漏洞、IBM Jazz for Service Management 跨站请求伪造漏洞。其中，“IBM Tivoli System Automation for Multiplatforms 本地权限提升漏洞、IBM PowerKVM 命令执行漏洞、IBM Tivoli Storage Manager Server 缓冲区溢出漏洞”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-2017-02623
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02624

http://www.cnvd.org.cn/flaw/show/CNVD-2017-02626
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02480
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02598
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02566
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02506
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02513

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，该产品被披露存在权限获取和拒绝服务漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Linux kernel 权限获取漏洞（CNVD-2017-02608）、Linux kernel 本地拒绝服务漏洞（CNVD-2017-02609、CNVD-2017-02605、CNVD-2017-02606、CNVD-2017-02607、CNVD-2017-02604、CNVD-2017-02602）、Linux kernel 拒绝服务漏洞（CNVD-2017-02483）。其中，“Linux kernel 权限获取漏洞（CNVD-2017-02608）、Linux kernel 本地拒绝服务漏洞（CNVD-2017-02606）”的综合评级为“高危”。目前，除“Linux kernel 本地拒绝服务漏洞（CNVD-2017-02606）”外，剩余漏洞已经发布了相应的修补程序。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-2017-02608
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02609
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02605
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02606
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02607
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02604
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02602
http://www.cnvd.org.cn/flaw/show/CNVD-2017-02483

5、多款 D-Link DGS-1510 Websmart 设备安全绕过漏洞

D-Link DGS-1510-28XMP 是友讯（D-Link）公司的以太网交换机。本周，D-Link 被披露存在安全绕过漏洞，攻击者可利用该漏洞提交特殊的请求，进行未授权的命令执行。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-2017-02485

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-201	GeniXCMS 安全绕过漏洞	高	用户可联系供应商获得补丁信息：

7-02444			https://github.com/semplon/GeniXCMS/issues/70
CNVD-2017-02450	Apple macOS 任意代码执行漏洞（CNVD-2017-02450）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://support.apple.com/en-us/HT207275
CNVD-2017-02458	PHP DEP Violation 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：et/ChangeLog-7.php
CNVD-2017-02466	IVPN Client for Windows 权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.ivpn.net/setup/windows-changelog.html
CNVD-2017-02540	Iceni Argus 内存破坏漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：http://www.iceni.com/legacy.htm
CNVD-2017-02553	rubyzip gem Zip::File 组件目录遍历漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://github.com/rubyzip/rubyzip/issues/315
CNVD-2017-02563	ytnef 缓冲区溢出拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/Yeraze/ytnef/pull/27
CNVD-2017-02586	WinPLC 栈缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.vipa.com/
CNVD-2017-02591	NETGEAR DGN2200 远程执行代码漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://kb.netgear.com/
CNVD-2017-02627	多款 D-Link 产品栈缓冲区溢出漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页：http://www.dlink.com/

表 5 部分重要高危漏洞列表

小结：本周，Apache Struts2 被披露存在 S2-045 远程代码执行漏洞，攻击者可利用漏洞直接取得网站服务器控制权。此外，Apple、IBM、Linux 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、进行跨站脚本攻击、执行任意代码或发起拒绝服务攻击等。另外，D-Link 被披露存在安全绕过漏洞，攻击者可利用该漏洞提交特殊的请求，进行未授权的命令执行。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. 大华科技 11 款摄像头产品被曝预留了后门，可远程获取管理员账户密码

最近，中国浙江的一家安全摄像头/DVR 制造商大华科技（Dahua Technology）针对旗下的不少产品推送了固件升级补丁。补丁据说是为了修复某些型号中的一个“严重漏洞”。但实际上，在这家公司发布补丁之前，就已经有安全专家爆料，这个所谓的“严重漏洞”实际上是厂商预留的一个后门。大华已经在官网上公布了受漏洞影响的设备，包括下表中的 11 款设备，用户应该检查一下自己的设备型号是否在其列，并下载相应设备固件，完成更新。

参考链接：http://www.freebuf.com/news/128963.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