国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 12 月 11 日-2017 年 12 月 17 日

2017 年第 51 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 211 个，其中高危漏洞 87 个、中危漏洞 100 个、低危漏洞 24 个。漏洞平均分值为 5.94 本周收录的漏洞中，涉及 0day 漏洞 54 个（占 26%），其中互联网上出现“PHP Scripts Mall Cab Booking Script SQL 注入漏洞”等零日代码攻击漏洞。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 567 个，与上周（648 个）环比减少 12%。

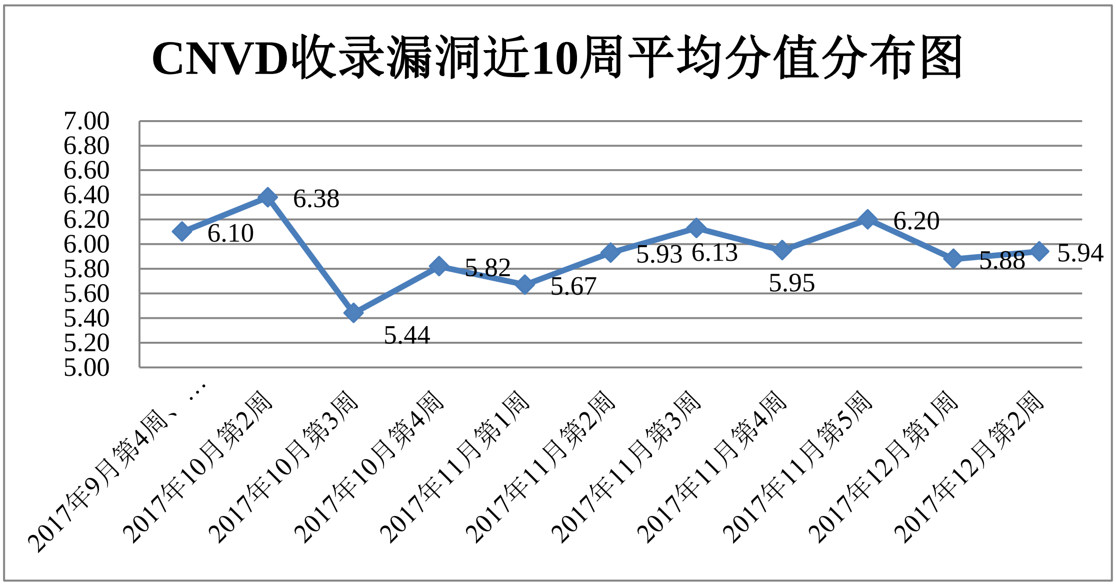

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，天融信、绿盟科技、安天实验室、中国电信集团系统集成有限责任公司、H3C 等单位报送数量较多。南京联成科技发展股份有限公司、中新网络信息安全股份有限公司、北京智游网安科技有限公司、网信智安、成都思维世纪科技有限公司、山石网科通信技术有限公司、广州非凡信息安全技术有限公司、君立

华域及其他个人白帽子向CNVD提交了567个以事件型漏洞为主的原创漏洞。

表1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
天融信	322	4
绿盟科技	237	0
360网神	220	220
安天实验室	211	0
中国电信集团系统集成有限责任公司	157	0
H3C	120	0
华为技术有限公司	93	0
蓝盾信息安全技术有限公司	91	0
启明星辰	71	0
恒安嘉新	70	0
杭州安恒信息技术有限公司	63	23
北京数字观星科技有限公司	30	0
漏洞盒子	11	11
知道创宇	3	0
南京联成科技发展股份有限公司	29	29
中新网络信息安全股份有限公司	9	9
北京智游网安科技有限公司	5	5
网信智安	2	2
成都思维世纪科技有限公司	2	2
山石网科通信技术有限公司	1	1

广州非凡信息安全技术有限公司	1	1
君立华域	1	1
CNCERT 新疆分中心	3	3
CNCERT 上海分中心	2	2
CNCERT 广东分中心	2	2
CNCERT 浙江分中心	2	2
个人	250	250
报送总计	2008	567

本周漏洞按类型和厂商统计

本周，CNVD 收录了 211 个漏洞。其中应用程序漏洞 97 个，操作系统漏洞 69 个，web 应用漏洞 28 个，安全产品漏洞 12 个，网络设备漏洞 5 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序漏洞	97
操作系统漏洞	69
web 应用漏洞	28
安全产品漏洞	12
网络设备漏洞	5

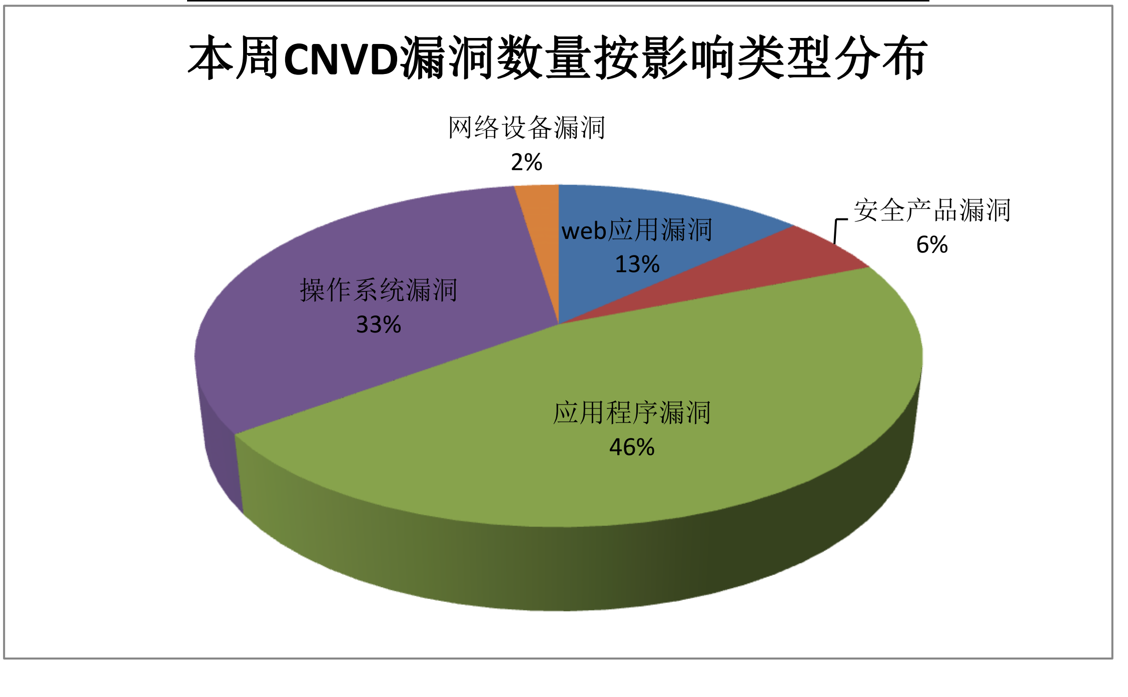

图 2 本周漏洞按影响类型分布

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

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Google	47	22%
2	Microsoft	22	10%
3	Adobe	18	9%
4	TG Soft	12	6%
5	SAP	9	4%
6	PHP	8	4%
7	ZOHO	6	3%
8	GraphicsMagick	5	2%
9	ImageMagick	5	2%
10	其他	79	38%

本周行业漏洞收录情况

本周，CNVD 收录了 1 个电信行业漏洞，50 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“多个 Phoenix Contact 产品跨站脚本漏洞、Apple watchOS IOSurface 组件内存破坏漏洞、多款 Siemens 产品拒绝服务漏洞、多款 Cisco 产品未授权访问漏洞、Google Android Kernel 组件权限提升漏洞”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/

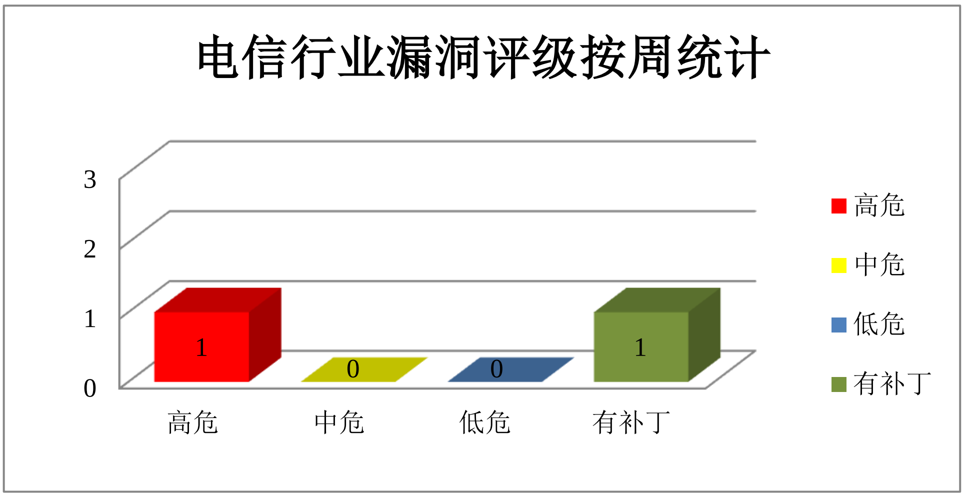

图 3 电信行业漏洞统计

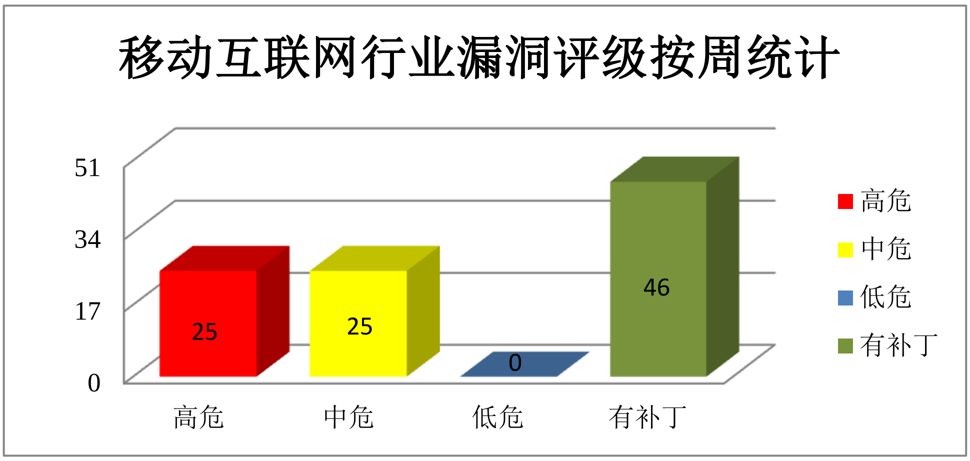

图 4 移动互联网行业漏洞统计

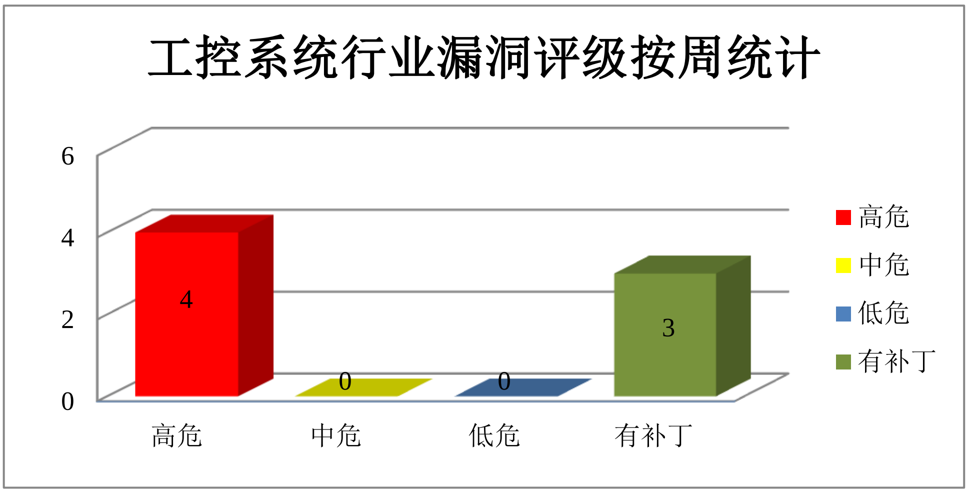

图 5 工控行业漏洞统计

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 Synapse 存在远程代码执行漏洞

Apache Synapse 是一个简单的、高质量开放源代码的替代方法。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Apache Synapse 远程代码执行漏洞。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-2017-36700

2、Palo Alto Networks 存在远程代码执行漏洞

Palo Alto Networks PAN-OS 是美国 Palo Alto Networks 公司为其防火墙设备开发的一套操作系统。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Palo Alto Networks PAN-OS 远程代码执行漏洞。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-2017-37056

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。NVIDIA driver 是使用在其中的美国英伟达（NVIDIA）公司开发的图形显卡驱动程序。MediaTek Display driver 是联发科（MediaTek）公司开发的显示驱动组件。Framework 是一个字体处理库。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android Framework 权限提升漏洞（CNVD-2017-36906、CNVD-2017-36907）、Google Android MediaTek 组件权限提升漏洞（CNVD-2017-36931、CNVD-2017-36932、CNVD-2017-36933）、Google Android NVIDIA 组件权限提升漏洞（CNVD-2017-36937、CNVD-2017-36938、CNVD-2017-36939）。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-2017-36906
http://www.cnvd.org.cn/flaw/show/CNVD-2017-36907
http://www.cnvd.org.cn/flaw/show/CNVD-2017-36931
http://www.cnvd.org.cn/flaw/show/CNVD-2017-36932
http://www.cnvd.org.cn/flaw/show/CNVD-2017-36933
http://www.cnvd.org.cn/flaw/show/CNVD-2017-36937
http://www.cnvd.org.cn/flaw/show/CNVD-2017-36938
http://www.cnvd.org.cn/flaw/show/CNVD-2017-36939

4、Microsoft 产品安全漏洞

Microsoft Excel 2016 是美国微软（Microsoft）公司 Office 套件中的一款电子表格

处理软件。Microsoft Office 2010 是一款办公软件套件。Microsoft Windows 7 SP1 等是一系列操作系统。Microsoft ASP.NET Core 是一个跨平台开源框架。本周，上述产品被披露存在权限提升、远程代码执行和拒绝服务漏洞，攻击者可利用漏洞提升权限、执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Microsoft ASP.NET Core 拒绝服务漏洞（CNVD-2017-37109、CNVD-2017-37113）、Microsoft Excel 2016 Click-to-Run 远程代码执行漏洞、Microsoft Office 远程代码执行漏洞（CNVD-2017-37106、CNVD-2017-37107）、Microsoft Windows Edge ChakraCore 远程代码执行漏洞、Microsoft Windows Internet Explorer 远程代码执行漏洞（CNVD-2017-37103）、Microsoft Windows Kernel 权限提升漏洞（CNVD-2017-37120）。除“Microsoft ASP.NET Core 拒绝服务漏洞（CNVD-2017-37109、CNVD-2017-37113）”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-2017-37109
http://www.cnvd.org.cn/flaw/show/CNVD-2017-37113
http://www.cnvd.org.cn/flaw/show/CNVD-2017-37105
http://www.cnvd.org.cn/flaw/show/CNVD-2017-37106
http://www.cnvd.org.cn/flaw/show/CNVD-2017-37107
http://www.cnvd.org.cn/flaw/show/CNVD-2017-37104
http://www.cnvd.org.cn/flaw/show/CNVD-2017-37103
http://www.cnvd.org.cn/flaw/show/CNVD-2017-37120

5、Xiongmai Technology IP Cameras and DVRs 堆栈缓冲区溢出漏洞

IP Cameras and DVRs 是雄迈信息技术有限公司（Xiongmai Technology）生产的一款 IP 摄像机和录像机。本周，Xiongmai Technology 被披露存在堆栈缓冲区溢出漏洞，攻击者可远程执行代码或使设备崩溃。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 -2017-36865

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-2017-36864	Apple watchOS IOSurface 组件内存破坏漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://support.apple.com/zh-cn/HT208325
CNVD-2017-36877	多个 Phoenix Contact 产品跨站脚本漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://cert.vde.com/de-de/advisories/vde-2017-004
CNVD-2017-37051	GraphicsMagick 'WriteOnePNGImage'函数堆缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://hg.code.sf.net/p/graphicsmagick/code/rev/5b8414c0d0c4
CNVD-2017-37052	GraphicsMagick 'ImportCMYKQuantumType'函数堆缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://hg.code.sf.net/p/graphicsmagick/code/rev/a9c425688397
CNVD-2017-37054	GraphicsMagick 'ImportRGBQuantumType'函数堆缓冲区越边界读取漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://hg.code.sf.net/p/graphicsmagick/code/rev/1366f2dd9931
CNVD-2017-37055	GraphicsMagick 'ImportGrayQuantumType'函数堆缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://hg.code.sf.net/p/graphicsmagick/code/rev/460ef5e858ad
CNVD-2017-37053	ImageMagick 'Magick_png_read_raw_profile'函数堆缓冲区溢出漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.imagemagick.org/download/beta/
CNVD-2017-37085	SAP Plant Connectivity 任意代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://blogs.sap.com/2017/12/12/sap-security-patch-day-december-2017/
CNVD-2017-37121	Adobe Flash Player 越边界读取漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://helpx.adobe.com/security/products/flash-player/apsb17-33.html
CNVD-2017-37178	collectd SNMP 插件拒绝服务漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/collectd/collectd/releases/tag/collectd-5.6.3

表 4 部分重要高危漏洞列表

小结：本周，Apache Synapse 被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。此外，Palo Alto Networks、Google、Microsoft 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意代码或发起拒绝服务攻击等。另外，Xiongmai Technology 被披露存在堆栈缓冲区溢出漏洞，攻击者可远程执行代码或使设备崩溃。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。

本周重要漏洞攻击验证情况

本周，CNVD 建议注意防范以下已公开漏洞攻击验证情况。

1、PHP Scripts Mall Cab Booking Script SQL 注入漏洞

验证描述

PHP Scripts Mall Cab Booking Script 是印度 PHP Scripts Mall 公司的一套基于 PHP 的出租车在线预定脚本。

PHP Scripts Mall Cab Booking Script 1.0 版本中存在 SQL 注入漏洞。远程攻击者可通过向/service-list 发送‘city’参数利用该漏洞注入 SQL 命令。

验证信息

POC 链接：https://packetstormsecurity.com/files/145291/Cab-Booking-Script-1.0-SQL-Injection.html

参考链接：http://www.cnvd.org.cn/flaw/show/CNVD -2017-37214

信息提供者

恒安嘉新(北京)科技股份公司

注：以上验证信息(方法)可能带有攻击性，仅供安全研究之用。请广大用户加强对漏洞的防范工作，尽快下载相关补丁。

本周漏洞要闻速递

1. 暗网出现史上最大数据库

日前，暗网监控公司 4iQ 发现暗网中出现了 高达 41 GB 的数据文件，其中包含 14 亿份以明文形式存储的账号邮箱和密码等登录凭证。研究人员认为，这是迄今为止“在暗网中发现的最大数据库”。此前，在暗网中出现的最大数据库是 Exploit.in 泄露的 5.93 亿账户以及 Onliner Spambot 泄露的 7.11 亿账户。事实上，此次 1.4 亿登录凭证的在暗网中出现并非是严格意义上的数据泄露，而是包含此前 252 起登录凭证泄漏事件的交互式汇总数据库合集，其中还包括用 README 文件展示的搜索工具和插件脚本。此外，还有一个名为“imported.log”的文件，列出了泄露来源。

参考链接：http://www.freebuf.com/news/156986.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