

国家信息安全漏洞共享平台(CNVD)

国家信息安全漏洞共享平台

信息安全漏洞周报

2016 年 08 月 15 日-2016 年 08 月 21 日

2016 年第 34 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 189 个，其中高危漏洞 81 个、中危漏洞 103 个、低危漏洞 5 个。漏洞平均分为 6.32 分。本周收录的漏洞中，涉及 0day 漏洞 52 个（占 28%）。其中互联网上出现“ZOHO Web NMS Framework 存在多个漏洞（CNVD-2016-06370、CNVD-2016-06371）”等零日漏洞，此外互联网上披露了应用广泛的网络服务器监控软件 zabbix 存在的高危漏洞，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 36 个。

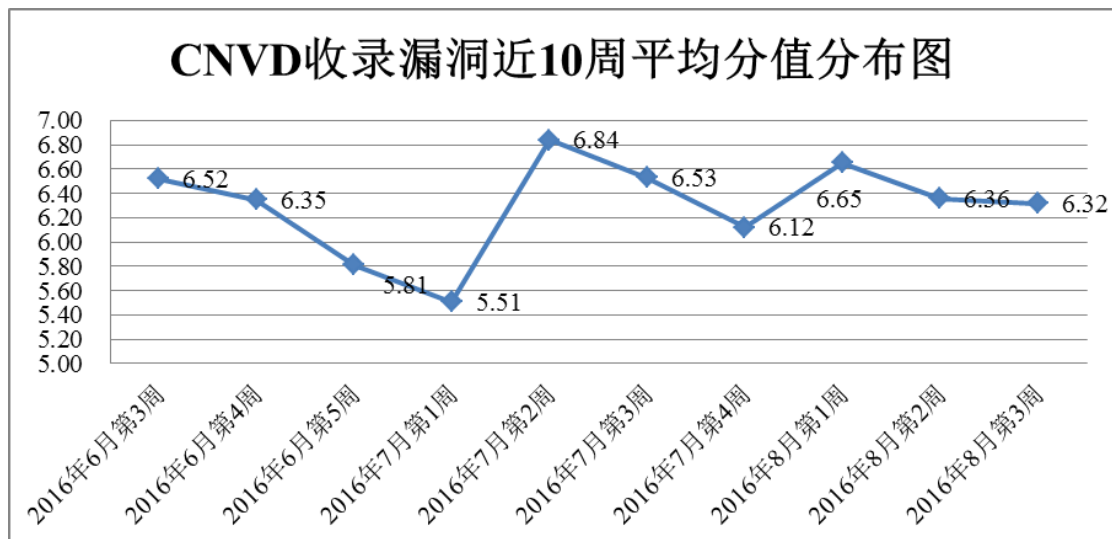


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 8 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 1

89 个漏洞。报送情况如表 1 所示。其中，安天实验室、恒安嘉新、东软、天融信等单位报送数量较多。漏洞盒子、北京安信天行科技有限公司、广州神月信息技术有限公司、中国航天科工四院软件评测中心、深圳市深信服电子科技有限公司及其他个人白帽子向 CNVD 提交了 36 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
安天实验室	121	0
恒安嘉新	118	0
东软	106	0
天融信	76	0
启明星辰	70	3
H3C	58	0
中国电信集团系统集成有限责任公司	33	0
杭州安恒信息技术有限公司	17	0
漏洞盒子	1	0
北京安信天行科技有限公司	5	5
广州神月信息技术有限公司	2	2
中国航天科工四院软件评测中心	1	1
深圳市深信服电子科技有限公司	1	1
CNCERT 宁夏分中心	2	2
个人	22	22
报送总计	633	36
录入总计	189（去重）	36

表 1 漏洞报送情况统计表

本周，CNVD 收录了 189 个漏洞。其中应用程序漏洞 135 个，网络设备漏洞 25 个，web 应用漏洞 13 个，安全产品 10 个，操作系统漏洞 4 个，数据库漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	135
网络设备漏洞	25
web 应用漏洞	13
安全产品漏洞	10
操作系统漏洞	4
数据库漏洞	2

表 2 漏洞按影响类型统计表

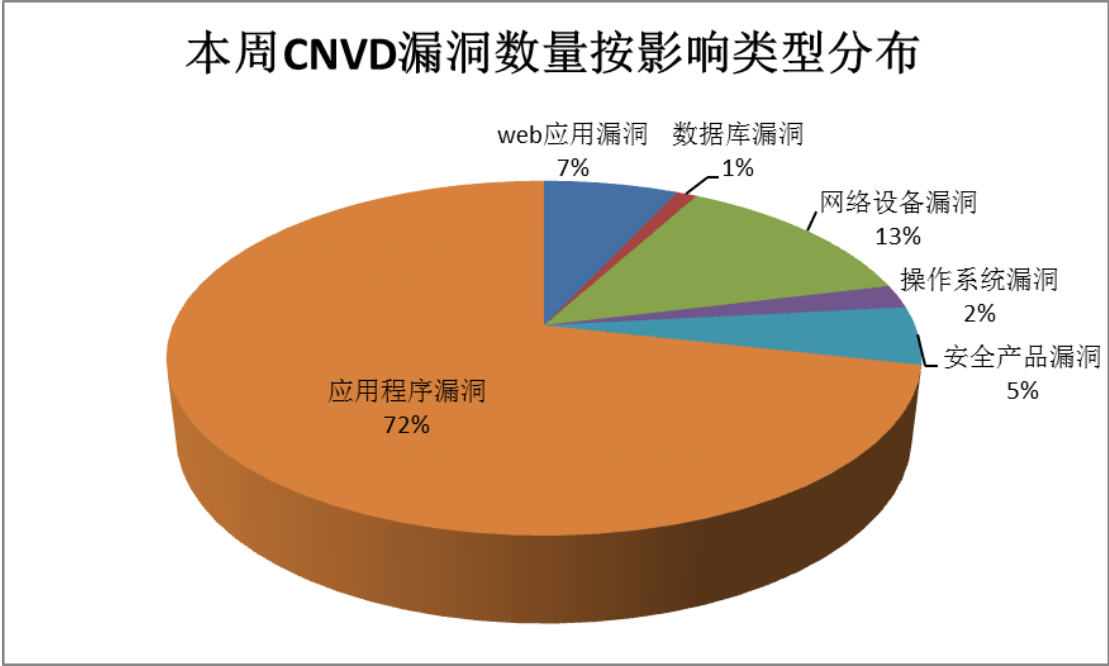


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、Cisco、Hancorn 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	IBM	25	13%
2	Cisco	17	9%
3	Hancorn	8	4%
4	PHP	7	4%
5	Fortinet	6	3%
6	SAP	5	3%
7	QEMU	5	3%

8	WSO2	5	3%
9	Cybozu	4	2%
10	其他	107	56%

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 7 个电信行业漏洞，1 个移动互联网行业漏洞（如下图所示）。其中，“Fortinet FortiGate 缓冲区溢出漏洞、PostgreSQL 本地提权漏洞、PostgreSQL 远程代码执行漏洞”的综合评级为“高危”。详情请参照 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/>

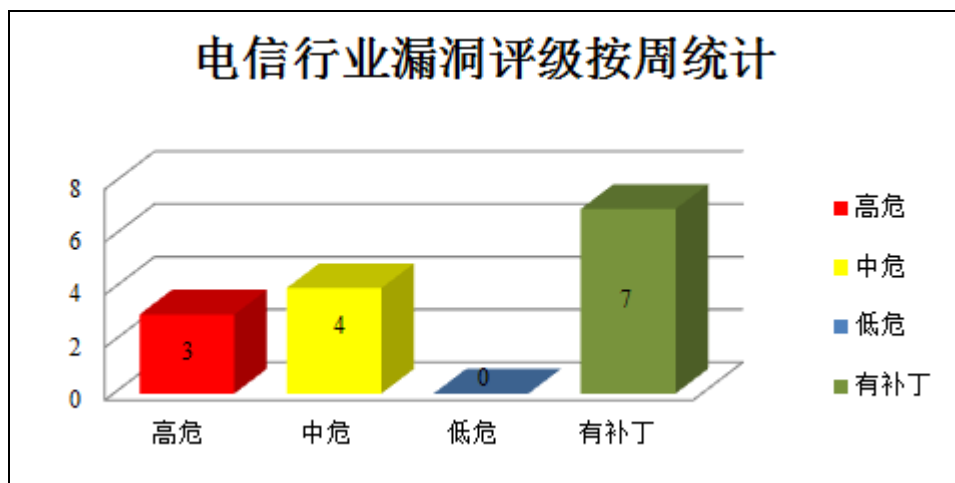


图 3 电信行业漏洞统计

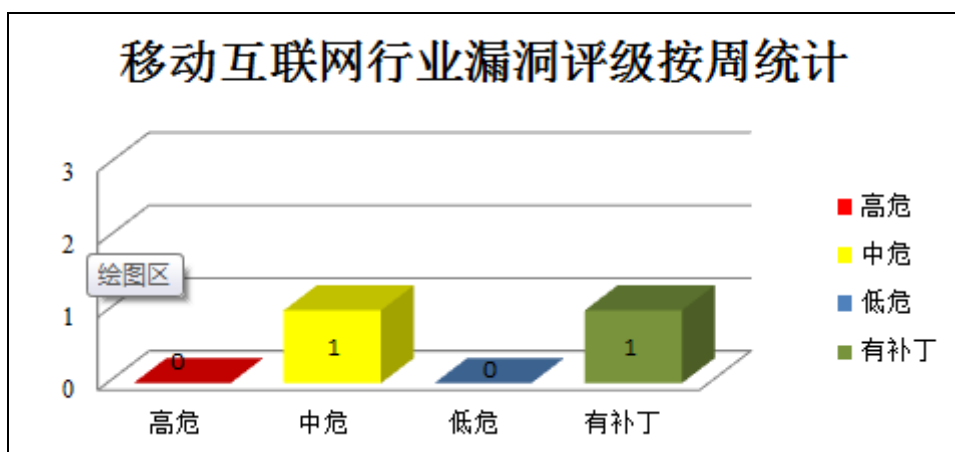


图 4 移动互联网行业漏洞统计

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、IBM 产品安全漏洞

IBM MQ Appliance 是一种解决方案，可支持 IBM MQ 部署于新用例，并简化现有部署选项，IBM BigFix 是美国 IBM 公司的一套系统管理软件，IBM API Connect 是一套用于管理 API 生命周期的集成解决方案，IBM NPM 是一套 NodeJS 包管理和分发工具，IBM Forms Experience Builder 是一套用于创建网站 Web 表单的应用程序，IBM Tivoli Monitoring (ITM) 是美国 IBM 公司的一套系统监控软件。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、执行任意命令或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：IBM MQ Appliance 本地命令执行漏洞、IBM BigFix x 平台操作系统命令注入漏洞、IBM BigFix Platform 中间人信息泄露漏洞、IBM API Connect 和 NPM 远程信息泄露漏洞、IBM Forms Experience Builder 跨站请求伪造漏洞、IBM Tivoli Monitoring Agent 栈缓冲区溢出漏洞、IBM BigFix WebReports 密码泄露漏洞、IBM BigFix 平台跨站请求伪造漏洞等。其中，除“IBM BigFix WebReports 密码泄露漏洞、IBM BigFix 平台跨站请求伪造漏洞”外漏洞的综合评级为“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-2016-06498>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06397>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06398>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06319>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06317>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06315>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06396>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06395>

2、Cisco 产品安全漏洞

Cisco Jabber for Windows 是美国思科 (Cisco) 公司的一套用于 Windows 平台的统一通信客户端解决方案。该方案提供了在线状态显示、即时消息、语音等功能。Cisco ASA 5500 系列自适应安全设备是用于提供安全和 VPN 服务的模块化平台，Cisco Firepower Management Center 和 Cisco ASA 5500-X Series with FirePOWER Services 都是美国思科 (Cisco) 公司的新一代防火墙软件。Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) 是一套提供了基于策略的用于自动配置端至端的基础设施控制器的应用程序，Cisco Aironet Access Points 是一套无线访问接入点设备。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、提升权

限或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco Jabber for Windows 任意代码执行漏洞、Cisco Adaptive Security Appliance Software 远程代码执行漏洞、Cisco Firepower Management Center 和 ASA 5500-X Series with FirePOWER Services 权限提升漏洞、Cisco Firepower Management Center 远程命令执行漏洞、Cisco Application Policy Infrastructure Controller Enterprise Module 远程代码执行漏洞、Cisco Aironet Access Points 平台拒绝服务漏洞、Cisco Aironet Access Points 平台拒绝服务漏洞（CNVD-2016-06435）、Cisco Aironet Access Points 平台提权漏洞等。其中，除“Cisco Aironet Access Points 平台拒绝服务漏洞、Cisco Aironet Access Points 平台拒绝服务漏洞（CNVD-2016-06435）、Cisco Aironet Access Points 平台提权漏洞”外漏洞的综合评级为“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-2016-06444>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06432>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06437>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06438>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06421>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06436>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06435>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06441>

3、Hancom 产品安全漏洞

Hancom Office 2014 VP 是韩国 Hancom 公司开发的一套云存储服务解决方案。本周，该产品被披露存在任意命令执行漏洞，攻击者可利用漏洞以应用程序上下文执行任意代码，或进行拒绝服务攻击。

CNVD 收录的相关漏洞包括：Hancom Office 2014 VP 本地任意代码执行漏洞（CNVD-2016-06351、CNVD-2016-06352、CNVD-2016-06353、CNVD-2016-06354、CNVD-2016-06355、CNVD-2016-06356、CNVD-2016-06357、CNVD-2016-06358）。上述漏洞的综合评级为“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-2016-06351>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06352>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06353>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06354>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06355>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06356>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06357>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06358>

4、PHP 产品安全漏洞

PHP 是一种开源的通用计算机脚本语言。本周，该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、执行任意代码和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：PHP 'ext/mcrypt/mcrypt.c'不完全修复存在多个整数溢出漏洞、PHP 'curl_escape()'函数整数溢出漏洞、PHP 'ext/calendar/calendar.c'缓冲区溢出漏洞、PHP 'ext/curl/interface.c'拒绝服务漏洞、PHP 'ext/exif/exif.c'信息泄露漏洞、PHP 'ext/mbstring/php_mbregex.c'缓冲区溢出漏洞、PHP 'php_snmp_parse_oid()'函数整数溢出漏洞。其中，除“PHP 'ext/curl/interface.c'拒绝服务漏洞、PHP 'curl_escape()'函数整数溢出漏洞、PHP 'ext/exif/exif.c'信息泄露漏洞”外漏洞的综合评级为“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-2016-06491>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06503>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06504>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06502>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06492>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06500>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06490>

5、ZOHO WebNMS Framework 存在多个漏洞

ZOHO WebNMS Framework 是美国卓豪（ZOHO）公司的一套用于构建网络管理应用的框架。本周，ZOHO WebNMS Framework 被披露存在目录遍历漏洞、信息泄露漏洞和用户冒充漏洞。攻击者可利用漏洞遍历目录、获取敏感信息、冒充任意用户和执行未授权操作。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-2016-06373>

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-2016-06316	BlueStacks 本地权限提升漏洞	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.bluestacks.cn/
CNVD-2016-06327	PostgreSQL 远程代码执行漏洞	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.postgresql.org/about/ne

			ws/1688/
CNVD-2016-06328	PostgreSQL 本地提权漏洞	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.postgresql.org/about/news/1688/
CNVD-2016-06363	SAP SAPCAR 本地提权漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://go.sap.com/
CNVD-2016-06364	SAP SAPCAR 本地提权漏洞（CNVD-2016-06364）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://go.sap.com/
CNVD-2016-06402	WSO2 Identity Server 存在多个漏洞	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://wso2.com/
CNVD-2016-06403	WSO2 Identity Server 存在多个漏洞（CNVD-2016-06403）	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://wso2.com/
CNVD-2016-06404	WSO2 Carbon 存在多个漏洞	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://wso2.com/
CNVD-2016-06405	WSO2 Carbon 存在多个漏洞（CNVD-2016-06405）	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://wso2.com/
CNVD-2016-06406	WSO2 Carbon 存在多个漏洞（CNVD-2016-06406）	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://wso2.com/

表 4 部分重要高危漏洞列表

小结：本周，IBM 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、执行任意命令或发起拒绝服务攻击等。此外，Cisco、Hancorn、PHP 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、执行任意代码和发起拒绝服务攻击等。另外，PostgreSQL 数据库软件被披露存在远程代码执行高危漏洞，攻击者可利用漏洞获得服务器管理权限。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. 漏洞预警：zabbix 再爆高危 SQL 注入漏洞，可获操作系统权限

zabbix 是一个开源的企业级性能监控解决方案。近日，zabbix 的 jsrpc 的 profileIdx 2 参数存在 insert 方式的 SQL 注入漏洞，攻击者无需授权登陆即可登陆 zabbix 管理系统，也可通过 script 等功能轻易直接获取 zabbix 服务器的操作系统权限。但是无需登录注入这里有个前提，就是 zabbix 开启了 guest 权限。而在 zabbix 中，guest 的默认密码为空。需要有这个条件的支持才可以进行无权限注入。尽快升级到最新版，3.0.4 版本已经修补。。

参考链接：<http://www.freebuf.com/vuls/112197.html>

2. 火狐、Chrome 皆中招：针对主流浏览器的网址欺诈漏洞

Baloch 披露了此漏洞，出现漏洞的主要原因是 Chrome 和 Android 版本的 Firefox 浏览器对某些 Unicode 字符的渲染不得当。阿拉伯语和希伯来语中会有一些字符是会从右到左显示的，比如“|”。当包含这种 Unicode 字符的 URL 和 IP 地址合在一起时，浏览器就会把 URL 从右到左显示。漏洞只存在于 Android 版本的 Firefox 浏览器，桌面版本不受影响，并且在 8 月 2 日的更新中已经修复了漏洞。

参考链接：<http://www.freebuf.com/vuls/112259.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