

信息安全漏洞周报

2017 年 11 月 13 日-2017 年 11 月 19 日

2017 年第 47 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 568 个，其中高危漏洞 204 个、中危漏洞 323 个、低危漏洞 41 个。漏洞平均分为 6.13。本周收录的漏洞中，涉及 0day 漏洞 104 个（占 18%），其中互联网上出现“Wordpress 插件 image-gallery-with-slideshow SQL 注入漏洞、EyesOfNetwork web interface SQL 注入漏洞”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 772 个，与上周（638 个）环比增长 21%。

CNVD收录漏洞近10周平均分分布图

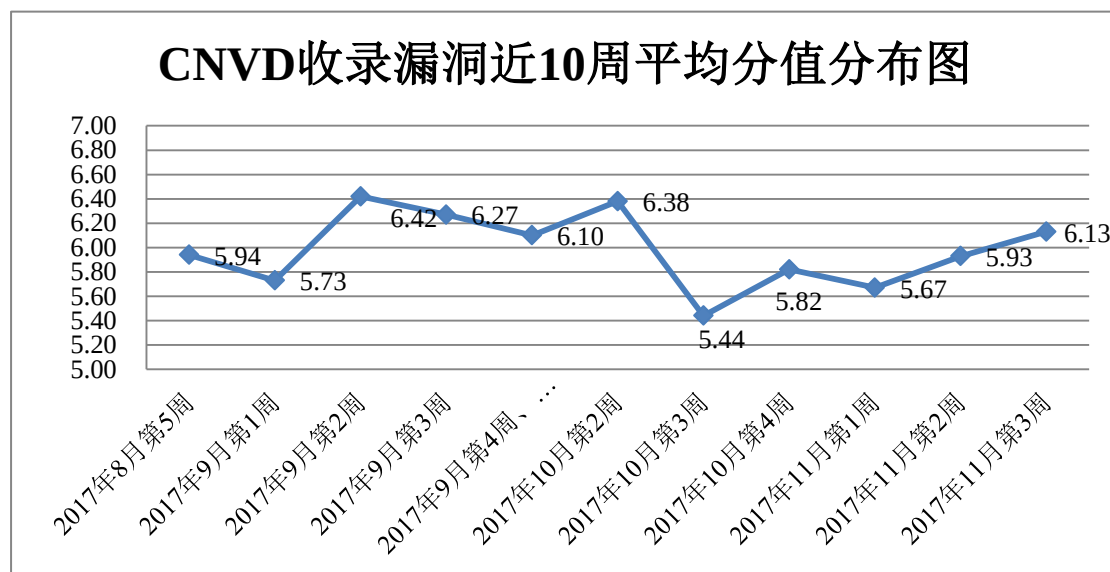


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，东软、启明星辰、H3C、华为技术有限公司、安天实验室等单位报送数量较多。聚锋信息安全实验室、深圳市鼎安天下信息科技有限公司、中新网络信息安全股份有限公司、四川虹微技术有限公司（子午攻防实验室）、聚

锋信息安全实验室、长沙天融信网络安全技术有限公司、福建榕基软件股份有限公司、广州软云计算机科技有限公司、南瑞集团公司（国网电力科学研究院）及其他个人白帽子向 CNVD 提交了 772 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
东软	262	1
启明星辰	259	0
H3C	225	2
华为技术有限公司	213	0
360 网神	207	207
安天实验室	202	0
漏洞盒子	168	168
恒安嘉新	114	0
绿盟科技	91	0
中国电信集团系统集成有 限责任公司	76	0
天融信	68	6
杭州安恒信息技术有限公 司	49	0
深圳市腾讯计算机系统有 限公司（玄武实验室）	19	19
广西鑫瀚科技有限公司	5	5
知道创宇	3	3
聚锋信息安全实验室	16	16
深圳市鼎安天下信息科技 有限公司	14	14
中新网络信息安全股份有 限公司	7	7
四川虹微技术有限公司 （子午攻防实验室）	6	6

聚锋信息安全实验室	3	3
长沙天融信网络安全技术有限公司	2	2
福建榕基软件股份有限公司	2	2
广州软云计算机科技有限公司	1	1
南瑞集团公司（国网电力科学研究院）	1	1
CNCERT 浙江分中心	5	5
CNCERT 广东分中心	2	2
CNCERT 新疆分中心	2	2
个人	300	300
报送总计	2322	772

本周漏洞按类型和厂商统计

本周，CNVD 收录了 568 个漏洞。其中应用程序漏洞 335 个，操作系统漏洞 92 个，web 应用漏洞 68 个，网络设备漏洞 67 个，数据库漏洞 3 个，安全产品漏洞 3 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	335
操作系统漏洞	92
web 应用漏洞	68
网络设备漏洞	67
安全产品漏洞	3
数据库漏洞	3

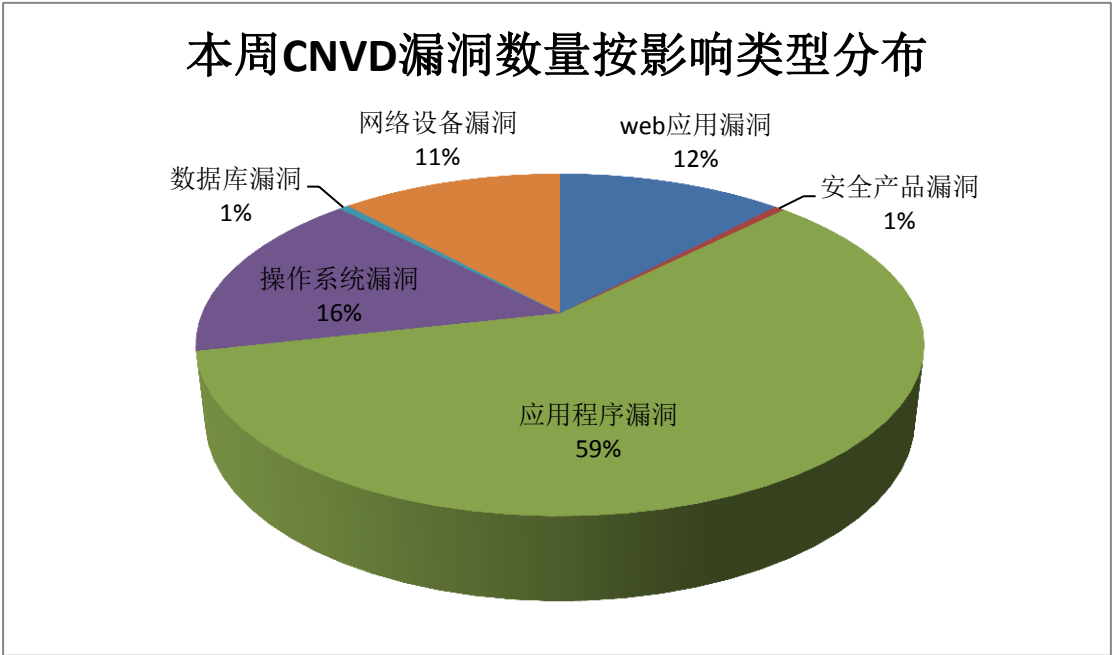


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、Huawei、IBM 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	Apple	77	14%
2	Huawei	37	7%
3	IBM	35	6%
4	Cisco	24	4%
5	Google	21	4%
6	Apache	20	4%
7	Oracle	18	3%
8	Foscam	12	2%
9	Microsoft	10	2%
10	其他	314	54%

本周行业漏洞收录情况

本周，CNVD 收录了 17 个电信行业漏洞，83 个移动互联网行业漏洞，11 个工控行业漏洞（如下图所示）。其中，“Cisco ASR 1000 未授权访问漏洞、NTT DOCOMO Wi-Fi STATION L-02F Software 存在后门漏洞、多款 Apple 产品 WebKit 代码执行漏洞、

多款 Moxa Nport 产品拒绝服务漏洞、SICAM RTU SM-2556 COM 模块任意代码执行漏洞”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/>

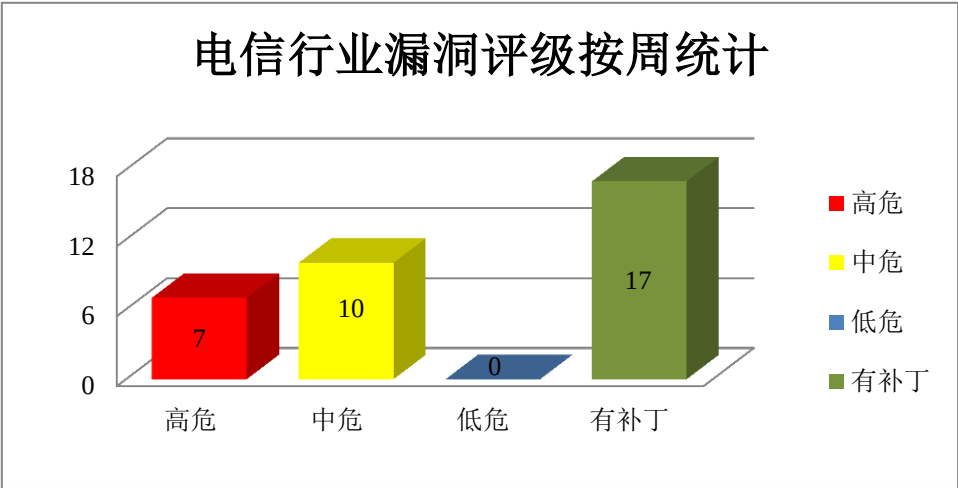


图 3 电信行业漏洞统计

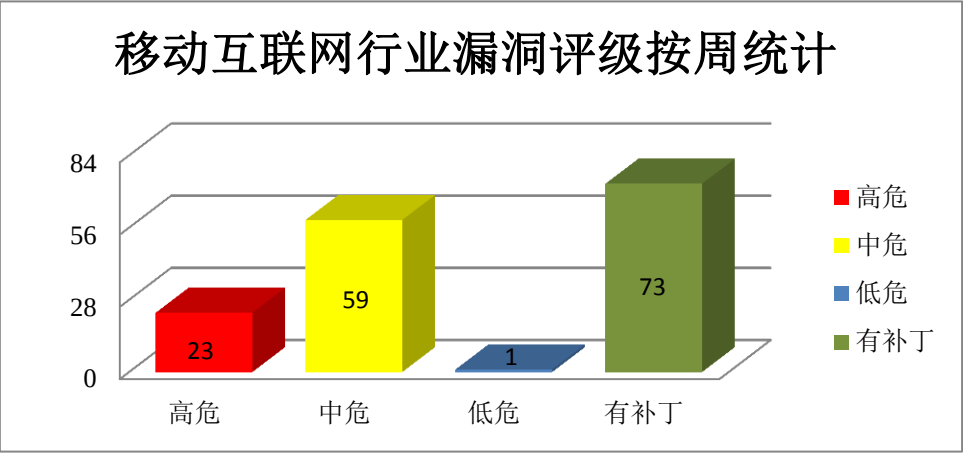


图 4 移动互联网行业漏洞统计

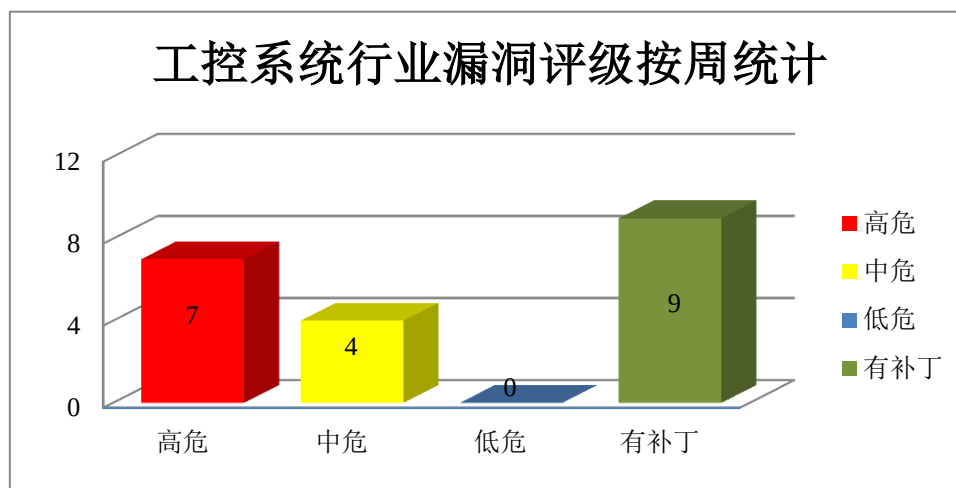


图 5 工控行业漏洞统计

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、Microsoft office 组件安全漏洞

Microsoft Office 是微软公司开发的一套基于 Windows 操作系统的办公软件套装。本周，该产品被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft office 组件 EQNEDT32.EXE 存在内存破坏漏洞。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-2017-34031>

2、Apple 产品安全漏洞

Apple iOS、iCloud for Windows、iTunes for Windows、Safari 和 tvOS 都是美国苹果（Apple）公司的产品。Apple iOS 是一套为专移动设备所开发的一套操作系统；Safari 是一款 Web 浏览器。WebKit 是其中的一个 Web 浏览器引擎组件。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：多款 Apple 产品 WebKit 内存破坏漏洞（CNVD-2017-34326、CNVD-2017-34327、CNVD-2017-34328、CNVD-2017-34329、CNVD-2017-34330、CNVD-2017-34331、CNVD-2017-34332、CNVD-2017-34333）。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-2017-34326>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34327>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34328>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34329>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34330>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34331>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34332>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34333>

3、Apache 产品安全漏洞

Apache CouchDB 是美国阿帕奇软件基金会的一个数据库。Apache Traffic Server 是一款 HTTP 代理和缓存服务器。Apache Storm 是一套分布式实时计算系统。本周，该产品被披露存在远程代码执行和目录遍历漏洞，攻击者可利用漏洞执行任意代码或读取任意文件。

CNVD 收录的相关漏洞包括：Apache Brooklyn 远程代码执行漏洞、Apache CouchDB 权限提升漏洞、Apache CouchDB 远程代码执行漏洞、Apache James java 反序列化任意命令执行漏洞、Apache OpenNLP XXE 漏洞、Apache Spark 反序列化的程代码执行漏洞、Apache Storm 目录遍历漏洞、Apache Traffic Server 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-2017-34168>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34233>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34234>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34170>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34181>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34169>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34236>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34469>

4、Huawei 产品安全漏洞

Huawei RP200 及 TE 系列及都是华为公司面向高端客户的一体化桌面智真产品及高清视频会议终端产品。Huawei FusionSphere 是基于 OpenStack 框架开发的云操作系统产品。Huawei ME906S-158 是一款笔记本电脑。Huawei UMA 是一款统一审计系统。Huawei VIE-L09 是华一款智能手机。本周，上述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注入攻击等。

CNVD 收录的相关漏洞包括：Huawei FusionSphere SQL 注入漏洞、Huawei FusionSphere 命令注入漏洞、Huawei ME906S 权限提升漏洞、Huawei UMA 产品 SQL 注入漏洞、Huawei VIE-L09 缓冲区溢出漏洞、多款 Huawei 产品越界读漏洞（CNVD-2017-34418、CNVD-2017-34419、CNVD-2017-34420）。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-2017-33878>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-33877>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34438>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34272>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34411>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34418>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34419>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-34420>

5、Philips IntelliSpace Cardiovascular System and Xcelera System 明文存储漏洞

Philips IntelliSpace Cardiovascular 和 Xcelera 系统是全面的心脏影像和信息管理软件。本周, Philips 被披露存在明文存储漏洞, 具有较高特权的攻击者获得对数据的未经授权访问, 包括患者健康信息, 系统资源和误用连接资产。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-2017-34035>

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-2017-33662	Interspire Email Marketer 安全绕过漏洞	高	用户可联系供应商获得补丁信息: http://www.exploitalert.com/view-details.html?id=27810
CNVD-2017-33738	GNU C Library 'glob'函数堆缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞, 详情请关注厂商主页: https://www.gnu.org
CNVD-2017-33749	Fortinet FortiClient 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏洞, 补丁获取链接: http://fortiguard.com/psirt/FG-IR-16-095
CNVD-2017-33792	多款 JustSystems 产品内存破坏漏洞	高	目前厂商已发布升级补丁以修复漏洞, 补丁获取链接: https://www.justsystems.com/jp/info/js17003.html
CNVD-2017-33809	Datto Windows Agent 命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞, 补丁获取链接: https://www.datto.com/partner-security-update-nov2017
CNVD-2017-33811	QNAP 远程命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞, 补丁获取链接: https://www.qnap.com/zh-hk/releasenotes/

CNVD-2017-33849	AnyDesk 劫持漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://download.anydesk.com/changelog.txt
CNVD-2017-34265	Foscam IP Video Camera 命令注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： http://www.foscam.com/downloads/index.html
CNVD-2017-34267	Foscam IP Video Camera 缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： http://www.foscam.com/downloads/index.html
CNVD-2017-34436	Samba 任意文件写入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://www.samba.org/samba/security/

表 4 部分重要高危漏洞列表

小结：本周，Microsoft office 组件被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码。此外，Apple、Apache、Huawei 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命令注入攻击等。另外，Philips 被披露存在明文存储漏洞，具有较高特权的攻击者获得对数据的未经授权访问，包括患者健康信息，系统资源和误用连接资产。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. 微软 Patch Tuesday 修复三则重要漏洞

微软在 Patch Tuesday 中修复了 53 个安全漏洞，涉及的产品包括 Windows 操作系统、Office、Internet Explorer、Microsoft Edge、ASP.NET Core、.NET Core 以及 Chakra Core 浏览器引擎。这其中包括三枚重要的漏洞，Windows EOT 字体引擎信息泄露漏洞(CVE-2017-11832)、Windows 内核信息泄露漏洞(CVE-2017-11853)，Microsoft Excel 安全功能绕过漏洞(CVE-2017-11877)。

参考链接：<http://www.freebuf.com/news/154083.html>

2. IBM X-Force 发现新型银行木马 IcedID

近日，IBM X-Force 研究团队在一项针对最近一系列攻击美国金融机构的案例中发现了一款新型银行木马，并将其命名为“IcedID”，该银行木马目前似乎还处于开发的初始阶段。像 TrickBoty 银行木马 和 Dridex 银行木马类似，IcedID 也可以使用 Web 注入（注入浏览器进程显示重叠在原页面上的虚假内容）和重定向攻击（安装本地代理

将用户重定向到恶意网站）技术来执行窃取受害者的财务数据。

参考链接：<http://www.freebuf.com/news/154179.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