国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 03 月 28 日-2016 年 04 月 03 日　　2016 年第 14 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 93 个，其中高危漏洞 22 个、中危漏洞 64 个、低危漏洞 7 个。漏洞平均分值为 5.79 分。本周收录的漏洞中，涉及 0day 漏洞 9 个（占 10%）。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 758 个，与上周（554 个）环比增长 37%。

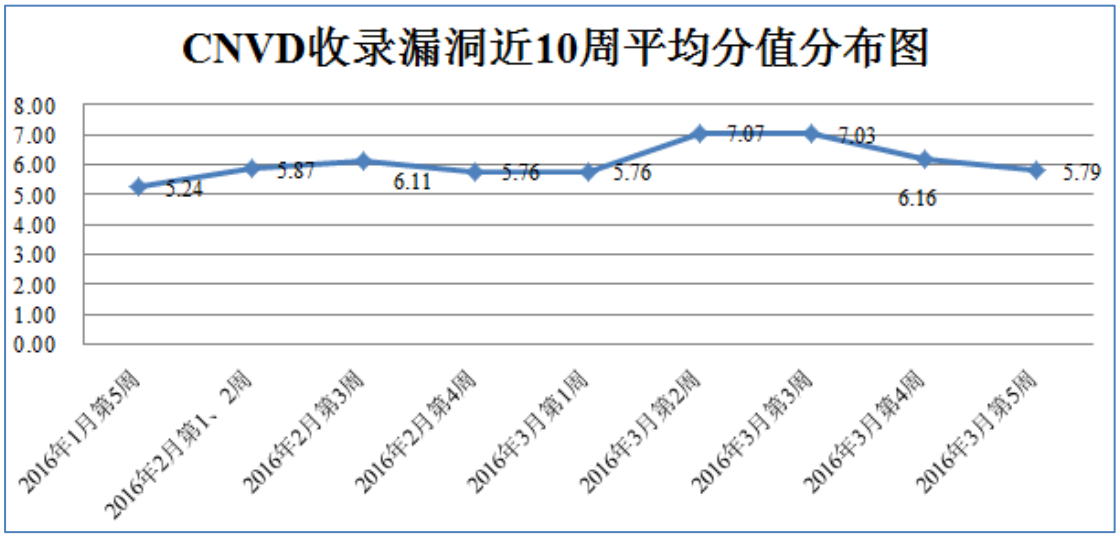

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 8 家成员单位、合作伙伴及个人报送了本周收录的全部 93 个漏洞。报送情况如表 1 所示。其中，启明星辰、天融信、安天实验室、绿盟科技等单位报送数量较多。补天平台、乌云、漏洞盒子、腾讯玄武实验室、腾讯电脑管家、High-Tech Bridge Security Research Lab、分中心及白帽子向 CNVD 提交了 758 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
奇虎(补天平台)	165	165
启明星辰	66	0
天融信	83	0
安天实验室	75	0
绿盟科技	67	0
恒安嘉新	37	1
东软	21	0
H3C	7	0
High-Tech Bridge Security Research Lab	3	3
乌云	506	506
漏洞盒子	26	26
腾讯玄武实验室	11	11
腾讯电脑管家	11	11
CNCERT 福建分中心	2	2
CNCERT 江西分中心	2	2
CNCERT 宁夏分中心	1	1
个人	30	30
报送总计	1113	758
录入总计	93（去重）	758

表 1 成员单位上报漏洞统计表

本周漏洞按类型和厂商统计

本周，CNVD 收录了 93 个漏洞。其中应用程序漏洞 57 个，Web 应用漏洞 15 个，操作系统漏洞 12 个，网络设备漏洞 8 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	57
Web 应用漏洞	15
操作系统漏洞	12
网络设备漏洞	8
安全产品漏洞	1

表 2 漏洞按影响类型统计表

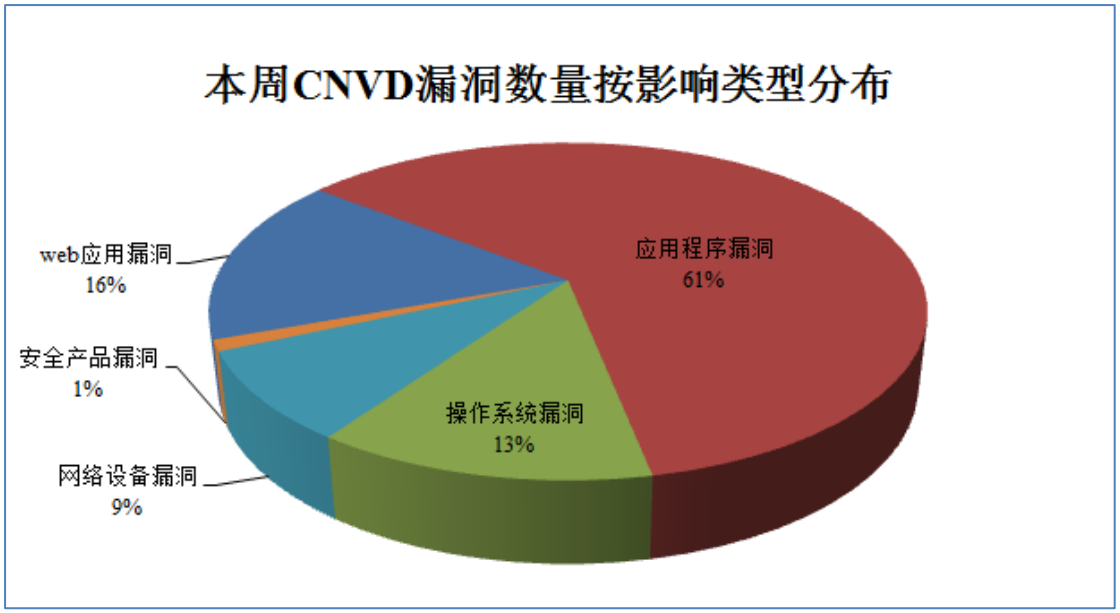

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Apple、Drupal、Cisco 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	Apple	11	12%
2	Drupal	10	11%
3	Cisco	9	10%
4	Google	6	6%
5	Apache	6	6%
6	QEMU	4	4%
7	CubeCart	3	3%
8	dhcpcd	3	3%
9	Foxit	3	3%
10	其他	38	42%

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 8 个电信行业漏洞、2 个移动互联网漏洞、1 个工控系统行业漏洞（如下图所示）。其中，“Cisco IOS Software Wide Area Application Services Express 拒绝服务漏洞、Cisco IOS 和 IOS XE Software DHCPv6 relay 拒绝服务漏洞、Cisco IOS Software 和 Cisco NX-OS Software Locator/ID Separation Protocol 拒绝服务漏洞、Cisco IOS/IOS XE/Cisco Unified Communications Manager 信息泄露漏洞、多款 Apple 产品 kernel 安全绕过漏洞、Cogent Real-Time Systems Cogent DataHub 提权漏洞”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/

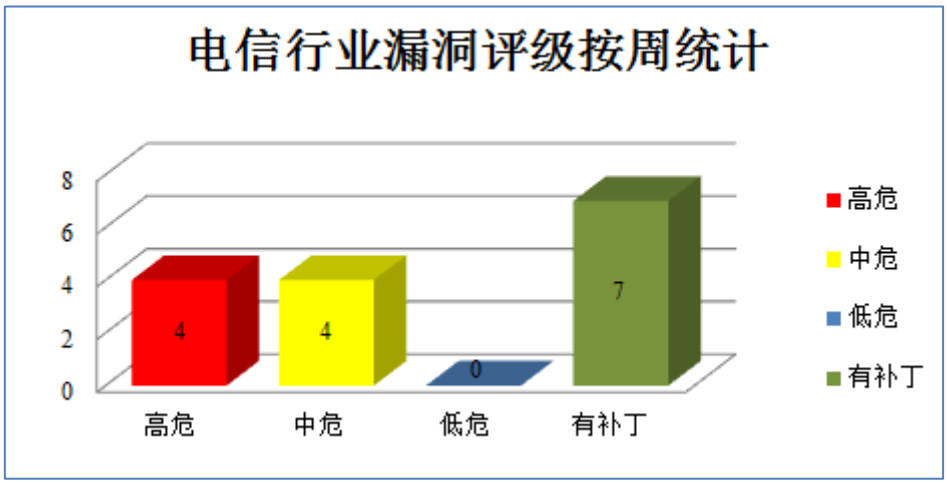

图 3 电信行业漏洞统计

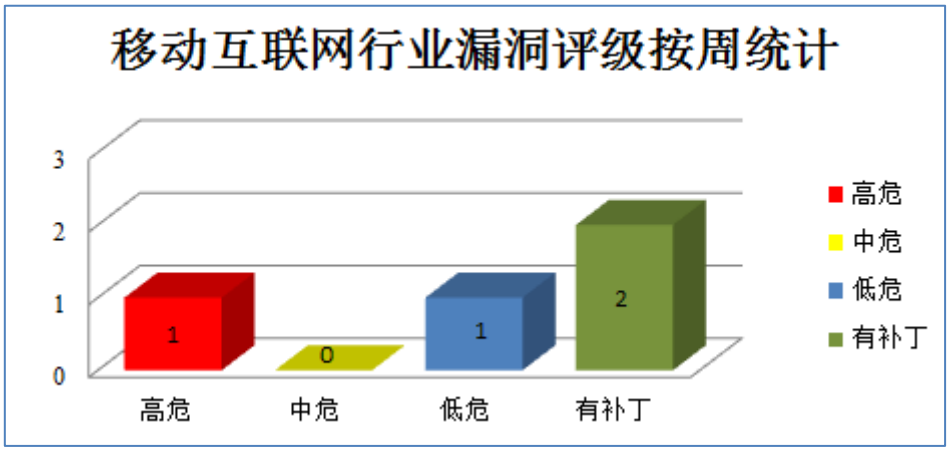

图 4 移动互联网行业漏洞统计

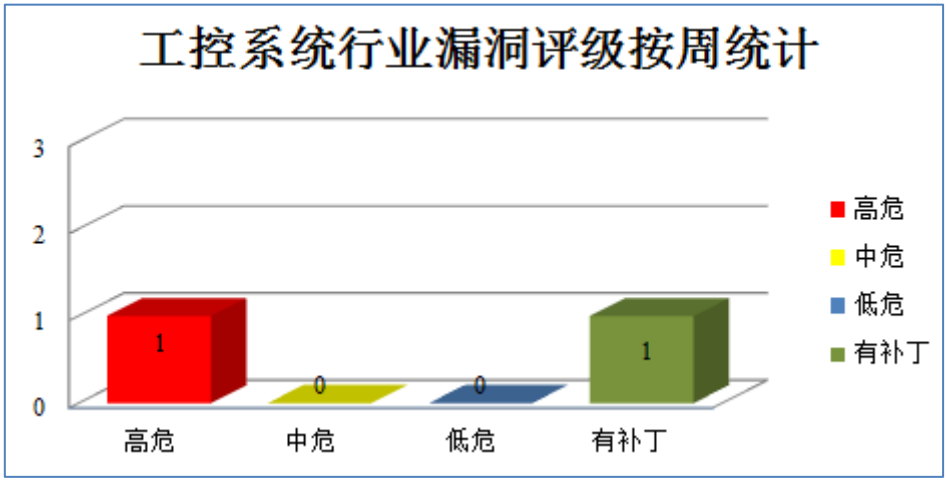

图 5 工控系统行业漏洞统计

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、 Google 产品安全漏洞

Google Chrome 是由 Google 开发的一款 Web 浏览工具。本周，该产品被披露存在内存错误引用和拒绝服务漏洞，允许攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Chrome V8 Array.prototype.concat 拒绝服务漏洞、Google Chrome RenderWidgetHostImpl::Destroy 内存错误引用漏洞、Google Chrome GetLoadTimes 内存错误引用漏洞、Google Chrome Program::getUniformInternal 拒绝服务漏洞、Google Chrome PageCaptureSaveAsMHTMLFunction::ReturnFailure 拒绝服务漏洞、Google Chrome V8 拒绝服务漏洞（CNVD-2016-01957）。除，“Google Chrome V8 拒绝服务漏洞（CNVD-2016-01957）”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-2016-01953

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01954

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01955

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01956

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01958

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01957

2、 Drupal 产品安全漏洞

Drupal 是一套用 PHP 语言开发的免费、开源的内容管理系统。本周，上述产品被披露存在多个安全漏洞，允许攻击者可利用漏洞获取敏感信息和执行任意代码等。

CNVD 收录的相关漏洞包括：Drupal Core 会话数据劫持漏洞、Drupal Core 反射文件下载漏洞、Drupal Core 双重编码'destination'参数开放重定向漏洞、Drupal Core HTTP 头注入漏洞、Drupal Core 形式接口忽略提交按钮访问限制漏洞、Drupal Core 开放重定向漏洞、Drupal Core 暴力放大攻击漏洞、Drupal Core File 模块存在多个漏洞等。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-2016-01930

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01933

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01934

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01935

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01936

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01937

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01938

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01939

3、 Apache 产品安全漏洞

Apache Ranger 是美国阿帕奇（Apache）软件基金会的一套为 Hadoop 群集实现全面安全措施的架构，它针对授权、结算和数据保护等核心企业安全要求，提供中央安全政策管理。Apache OpenMeetings 是美国阿帕奇（Apache）软件基金会所研发的一套多语言可定制的视频会议和协作系统，它支持音频、视频并允许用户查看每个与会者的桌面等。Apache Qpid 是 Apache 软件基金会开发的一款面向对象的消息中间件，Proton python API 是一个支持 python 语言并实现了 AMQP 1.0 协议的 API。本周，该上述产品被披露存在多个安全漏洞，远程攻击者可利用漏洞执行任意代码、进行跨站脚本攻击和读取任意文件等。

CNVD 收录的相关漏洞包括：Apache Ranger 未授权操作漏洞、ApacheOpenMeetingsOpenMeetings Administration 菜单目录遍历漏洞、Apache OpenMeetings 密码泄露漏洞、Apache OpenMeetings 跨站脚本漏洞、Apache OpenMeetingsFileService 任意文件读取漏洞、Apache Qpid Proton python API 明文传输漏洞。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-2016-01923

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01912

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01913

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01914

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01915

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01908

4、QEMU 产品安全漏洞

QEMU 是法国程序员法布里斯-贝拉（Fabrice Bellard）所研发的一套模拟处理器软件。该软件具有速度快、跨平台等特点。本周，该产品被披露存在整数溢出和拒绝服务漏洞，攻击者利用漏洞可获取敏感信息和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：QEMU 'ne2000_buffer_full()'拒绝服务漏洞、QEMU USB Net NDIS 整数溢出漏洞、QEMU 拒绝服务漏洞（CNVD-2016-01944、CNVD-2016-01943）。目前，厂商已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-2016-01946

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01945

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01944

http://www.cnvd.org.cn/flaw/show/CNVD-2016-01943

5、Red Hat Wildfly 信息泄露漏洞

Red Hat Wildfly（前称 JBoss Application Server）是美国红帽（Red Hat）公司的一款基于 JavaEE 的开源应用服务器。本周，Red Hat Wildfly 被披露存在信息泄露漏洞，攻击者可利用漏洞绕过过滤器限制。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-2016-01891

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-2016-01894	Cogent Real-Time Systems Cogent DataHub 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，详情请关注厂商主页：http://www.cogentdatahub.com/
CNVD-2016-01902	Apple 图形内核驱动权限提升漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://support.apple.com/HT206167
CNVD-2016-01904	Foxit Reader 和 Foxit PhantomPDF 远程代码执行漏洞	高	可参考厂商在 2016 年 3 月 16 日提供的安全补丁以修复该漏洞，厂商安全公告：https://www.foxitsoftware.com/support/security-bulletins.php
CNVD-2016-01906	Cisco IOS 和 IOS XE Software DHCPv6 relay 拒绝服务漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-dhcpv6

CNVD-2016-01920	Cisco IOS 和 IOS XE Software Internet Key Exchange 拒绝服务漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160323-ios-ikev2
CNVD-2016-01925	Autodesk Backburner 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这个安全问题，请到厂商的主页下载：https://knowledge.autodesk.com/support/3ds-max/troubleshooting/caas/CloudHelp/cloudhelp/2016/ENU/Installation-3DSMax/files/GUID-F6732A30-821C-4547-9FAA-E46BCA13392A-htm.html
CNVD-2016-01960	BMC Software BladeLogic Server Automation Suite RSCD Agent 密码重置漏洞	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://selfservice.bmc.com/casemgmt/sc_KnowledgeArticle?sfdcid=kA214000000dBpnCAE&type=Solution
CNVD-2016-01966	OpenELEC 和 RasPlex 权限获取漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：http://wiki.openelec.tv/
CNVD-2016-01967	Atlassian Bamboo Ignite Realtime Smack XMPP API 任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://jira.atlassian.com/browse/BAM-17099
CNVD-2016-01968	Atlassian Bamboo 任意代码执行漏洞	高	目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：https://jira.atlassian.com/browse/BAM-17101

表 4 部分重要高危漏洞列表

小结：本周，Google 产品被披露存在内存错误引用和拒绝服务漏洞，允许攻击者可利用漏洞发起拒绝服务攻击。此外，Drupal、Apache、QEMU 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息、进行跨站脚本攻击、执行任意代码和发起拒绝服务攻击等。另外，Red Hat Wildfly 被披露存在一个信息泄露漏洞，攻击者可利用漏洞绕过过滤器限制。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. Elasticsearch 目录遍历漏洞

Elasticsearch 是荷兰 Elasticsearch 公司的一套基于全文搜索引擎 Apache Lucene 构建的开源分布式 RESTful 搜索引擎，它主要用于云计算中，并支持通过 HTTP 使用 JSON 进行数据索引。该漏洞源于程序未能充分过滤用户提交的输入，远程攻击者可借助目录遍历字符‘..’利用该漏洞访问包含敏感信息的任意文件。

参考链接：http://www.freebuf.com/vuls/99942.html

2. 应用 Truecaller 存在远程利用漏洞

猎豹移动安全研究实验室的安全研究人员发现呼叫管理应用程序 Truecaller 存在严重漏洞。该漏洞允许任何人窃取 Truecaller 用户的敏感信息，为攻击者实施攻击提供条件。总体来说，一亿多已在智能手机上下载该应用程序的 Android 用户正处于危险之中。研究人员发现，Truecaller 使用设备的 IMEI 作为其用户的唯一身份认证标签。这意味着任何人只要获得了设备的 IMEI 就能得到 Truecaller 用户的个人信息（包括电话号码、家庭地址、邮箱、性别等），并且在没有用户的同意下，可以任意篡改用户的 APP 设置，将真正的用户暴露于恶意钓鱼者的威胁下。

参考链接：http://www.freebuf.com/vuls/100103.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