

信息安全漏洞周报

2017 年 06 月 26 日-2017 年 07 月 02 日

2017 年第 27 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 307 个，其中高危漏洞 104 个、中危漏洞 173 个、低危漏洞 30 个。漏洞平均分为 5.94。本周收录的漏洞中，涉及 0day 漏洞 79 个（占 26%），其中互联网上出现“libcroco 拒绝服务漏洞（CNVD-2017-11760）、DNSTracer 栈缓冲区溢出漏洞”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总数 1466 个，与上周（1336 个）环比增长 10%。

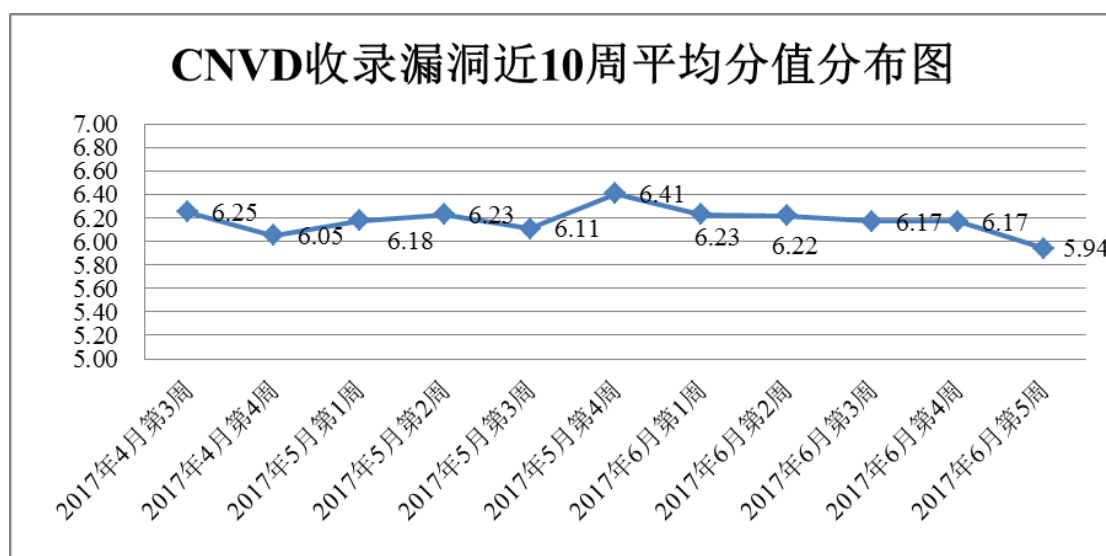


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 19 家成员单位、企业用户及个人用户报送了本周收录的全部 307 个漏洞。报送情况如表 1 所示。其中，安天实验室、阿里云计算有限公司、华为技术有限公司、天融信、启明星辰等单位报送数量较多。360 网神、漏洞盒子、福建六壬网安股份有限

公司、南京联成科技发展股份有限公司、广州神月信息技术有限公司、清远职业技术学院、广州软云计算科技有限公司、杭州朔方信息技术有限公司、河北网信智安信息技术有限公司、中新网络信息安全股份有限公司、中电长城网际系统应用有限公司、江苏君立华域信息技术有限公司、江苏同袍信息科技有限公司、华讯方舟股份有限公司、安徽新华博信息技术股份有限公司、北京山石网科信息技术有限公司、上海彝众信息技术有限公司及其他个人白帽子向 CNVD 提交了 1466 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
360 网神	275	275
安天实验室	166	0
阿里云计算有限公司	155	155
华为技术有限公司	105	0
天融信	78	2
漏洞盒子	77	77
启明星辰	77	5
H3C	75	0
恒安嘉新	73	0
绿盟科技	52	0
中国电信集团系统集成有限责任公司	48	0
杭州安恒信息技术有限公司	47	0
厦门服云信息科技有限公司	14	0
北京数字观星科技有限公司	5	0
东软	4	0
南京铤迅信息技术股份有限公司	2	2
广西鑫瀚科技有限公司	2	2

沈阳东软系统集成工程有限公司	1	1
西安四叶草信息技术有限公司	1	1
福建六壬网安股份有限公司	44	44
南京联成科技发展有限公司	39	39
广州神月信息安全技术有限公司	29	29
清远职业技术学院	24	24
广州软云计算机科技有限公司	19	19
杭州朔方信息技术有限公司	12	12
河北网信智安信息技术有限公司	12	12
中新网络信息安全股份有限公司	11	11
中电长城网际系统应用有限公司	10	10
江苏君立华域信息安全技术有限公司	8	8
江苏同袍信息科技有限公司	7	7
华讯方舟股份有限公司	5	5
安徽新华博信息技术股份有限公司	4	4
北京山石网科信息技术有限公司	2	2
上海彝众信息技术有限公司	2	2
吉林分中心	3	3
宁夏分中心	1	1
陕西分中心	1	1
个人	713	713
报送总计	2203	1466

录入总计	307（去重）	1466
------	---------	------

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 307 个漏洞。其中应用程序漏洞 179 个，web 应用漏洞 57 个，操作系统漏洞 48 个，网络设备漏洞 17 个，安全产品漏洞 5 个，数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	179
web 应用漏洞	57
操作系统漏洞	48
网络设备漏洞	17
安全产品漏洞	5
数据库漏洞	1

表 2 漏洞按影响类型统计表

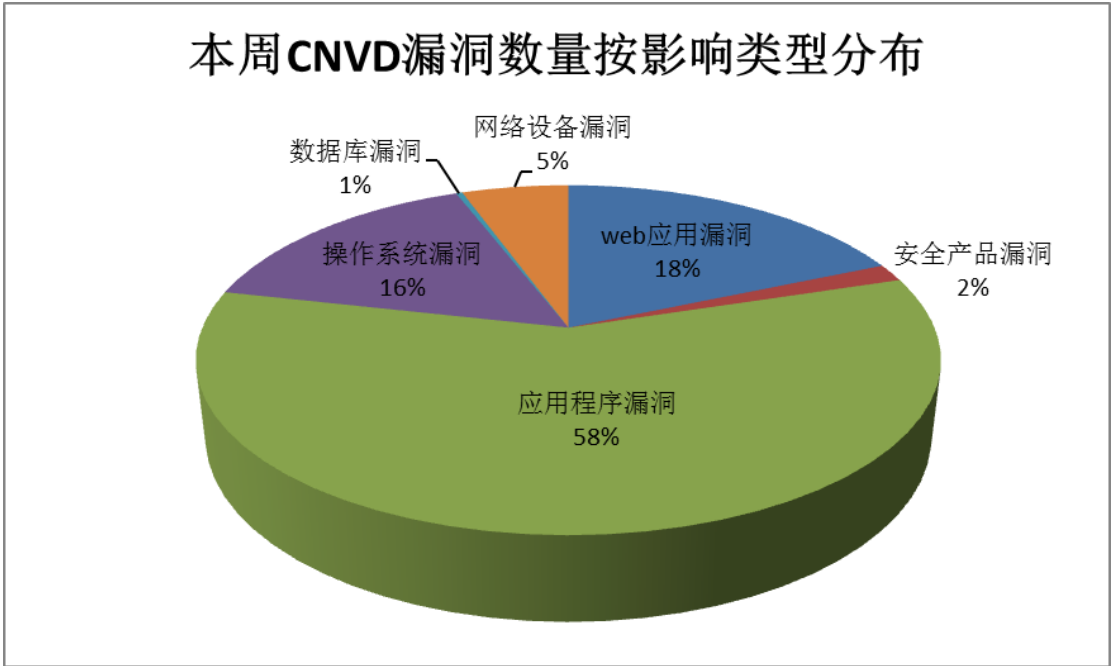


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft 、Google、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	Microsoft	45	15%
2	Google	26	8%
3	Cisco	22	7%

4	GNU	15	5%
5	IBM	14	5%
6	FAAD2	11	4%
7	libquicktime	7	2%
8	Elasticsearch	6	2%
9	Pivotal	5	2%
10	其他	157	50%

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 10 个电信行业漏洞，36 个移动互联网行业漏洞（如下图所示）。其中，“Cisco IOS XR Software 权限提升漏洞、Cisco IOS XR Software 本地命令注入漏洞、Cisco Ultra Services Framework Element Manager 默认密码漏洞、Google Android 内存访问漏洞、Huawei Y6 Pro graphics 驱动缓冲区溢出漏洞、Google Android 绕过身份验证漏洞、Google Android 未授权操作漏洞（CNVD-2017-11472）、Google Android 系统服务 ContentService 存在空对象引用漏洞”等的综合评级为“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/>

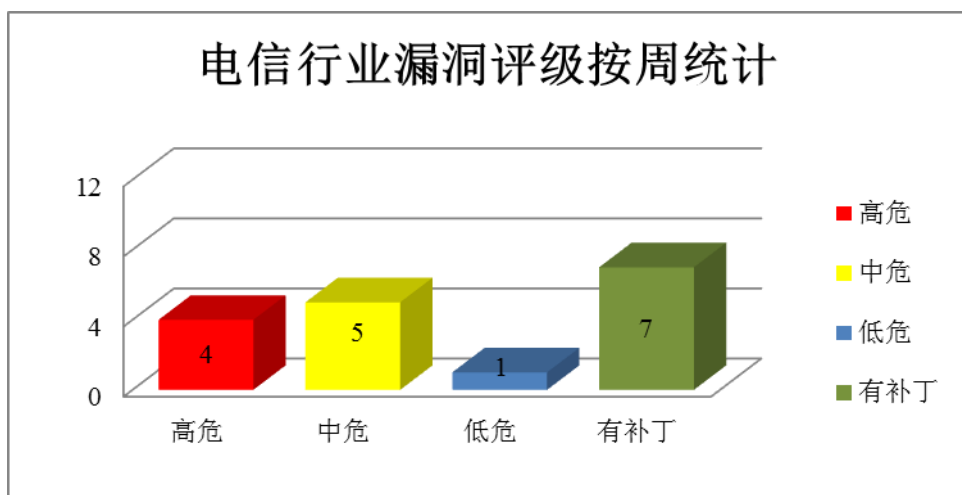


图 3 电信行业漏洞统计

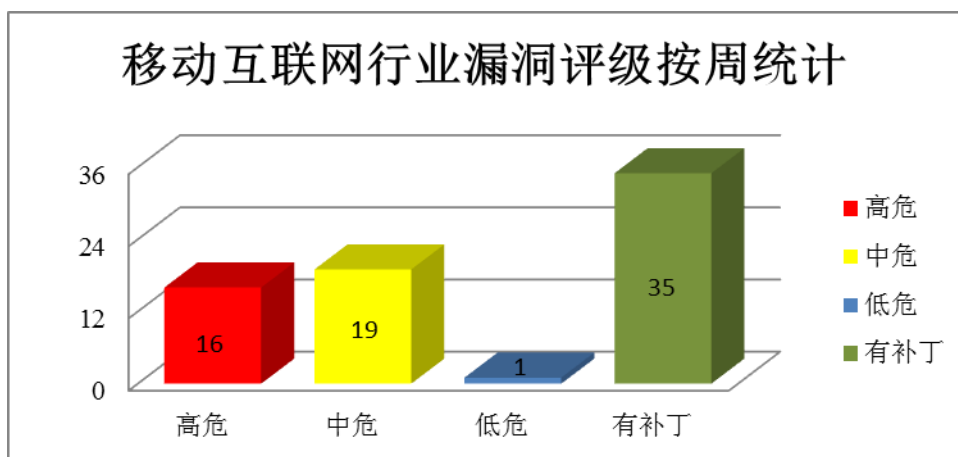


图 4 移动互联网行业漏洞统计

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 产品安全漏洞

Microsoft Office 是美国微软（Microsoft）公司开发的一款办公软件套件产品。Microsoft Edge 是一款 Windows 10 操作系统附带的默认浏览器。本周，上述产品被披露存在内存破坏和远程代码执行漏洞，攻击者可利用漏洞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 Office 远程代码执行漏洞（CNVD-2017-11786、CNVD-2017-11787、CNVD-2017-11788、CNVD-2017-11789、CNVD-2017-11790、CNVD-2017-11791）、Microsoft Edge 远程内存破坏漏洞（CNVD-2017-12092、CNVD-2017-12096）。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-2017-11786>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11787>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11788>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11789>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11790>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11791>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12092>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-12096>

2、Google 产品安全漏洞

Android 是美国谷歌（Google）公司和开放手持设备联盟共同开发的一套以 Linux 为基础的开源操作系统。Qualcomm 是使用在其中的一个设备专用的高通组件。本周，该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 Qualcomm 权限提升漏洞（CNVD-2017-11361、CNVD-2017-11362、CNVD-2017-11363、CNVD-2017-11364、CNVD-2017-11365、CNVD-2017-11366、CNVD-2017-11367、CNVD-2017-11368）。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-2017-11361>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11362>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11363>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11364>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11365>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11366>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11367>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11368>

3、Cisco 产品安全漏洞

Cisco IOS XR Software 是美国思科（Cisco）公司的 IOS 软件系列中的一套完全模块化、分布式的网络操作系统。Cisco Prime Collaboration 是综合性视频及声音服务保障及管理系统。Cisco Ultra Services Framework 是一个智能在线服务支付平台。Cisco Elastic Services Controller 是云及系统管理解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制、泄露敏感信息、执行任意代码或下载任意文件等。

CNVD 收录的相关漏洞包括：Cisco Elastic Services Controller 安全限制绕过漏洞、Cisco Elastic Services Controller 任意命令执行漏洞、Cisco IOS XR Software 本地命令注入漏洞、Cisco IOS XR Software 权限提升漏洞、Cisco Prime Collaboration Provisioning 任意文件下载漏洞、Cisco Ultra Services Framework Element Manager 默认密码漏洞、Cisco Elastic Services Controller 信息泄露漏洞、Cisco Elastic Services Controller 远程命令执行漏洞。除“Cisco Elastic Services Controller 信息泄露漏洞、Cisco Elastic Services Controller 远程命令执行漏洞”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-2017-11584>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11582>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11545>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11304>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11552>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11858>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11585>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11581>

4、Huawei 产品安全漏洞

Huawei nova、Y6 Pro 等都是中国华为（Huawei）公司的智能手机设备。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限或执行任意代码等。

CNVD 收录的相关漏洞包括：Huawei nova 青春版手机权限提升漏洞、Huawei Y6 Pro graphics 驱动内存泄露漏洞、Huawei Y6 Pro graphics 驱动缓冲区溢出漏洞、华为手机 TEE 模块 Use After Free 漏洞。其中“Huawei Y6 Pro graphics 驱动缓冲区溢出漏洞”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-2017-12111>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11751>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11752>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-11785>

5、Moxa AWK-3131A Wireless Access Point 操作系统命令注入漏洞

Moxa AWK-3131A Wireless Access Point 是中国摩莎（Moxa）公司的一款无线交换机。本周，Moxa 被披露存在命令注入漏洞，攻击者可利用漏洞控制受影响设备。目前，互联网上已经出现了针对该漏洞的攻击代码，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-2017-11314>

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-2017-11307	Drupal Core 远程代码执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： https://www.drupal.org/SA-CORE-2017-003
CNVD-2017-11309	CompuLab Intense PC 和 MintBox 2 BIOS 权限漏洞	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： http://compulab.com/
CNVD-2017-11317	Sudo 输入验证漏洞（CNVD-2017-11317）	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.sudo.ws/alerts/linux_tty.html
CNVD-2017-11647	FreeRADIUS 安全绕过漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接： http://freeradius.org/security.html
CNVD-201	Canonical Juju 权限提升漏洞	高	目前厂商已发布升级补丁以修复漏

7-11648			洞，详情请关注厂商主页： https://jujucharms.com/
CNVD-2017-11961	Xen XSA-222 权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： http://seclists.org/oss-sec/2017/q2/520
CNVD-2017-11958	Xen Page Transfer 'xen/arch/x86/mm.c'权限提升漏洞	高	厂商已发布漏洞修复程序，请及时关注更新： http://seclists.org/oss-sec/2017/q2/517
CNVD-2017-12112	Siemens ViewPort for Web Office Portal 远程代码执行漏洞	高	用户可联系供应商获得补丁信息： https://www.siemens.com/cert/advisories/
CNVD-2017-12212	JAD Java Decompiler 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://varanekas.com/jad/
CNVD-2017-12211	Octopus Deploy 认证代码执行漏洞	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://octopus.com/downloads

表 4 部分重要高危漏洞列表

小结：本周，Microsoft 被披露存在内存破坏和远程代码执行漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。此外，Google、Cisco、Huwei 等多款产品被披露存在多个漏洞，攻击者利用漏洞可绕过安全限制、提升权限、执行任意命令或泄露敏感信息等。另外，Moxa 被披露存在命令注入漏洞，攻击者可利用漏洞控制受影响设备。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. FFmpeg 曝任意文件读取漏洞

6 月 24 日，HackerOne 平台名为 neex 的白帽子针对俄罗斯最大社交网站 VK.com 上报了该漏洞。ffmpeg 可处理 HLS 播放列表，而播放列表中已知可包含外部文件的援引。neex 表示他借由该特性，利用 avi 文件中的 GAB2 字幕块，可以通过 XBIN codec 获取到视频转换网站的本地文件。用户可以通过升级受影响版本至 FFmpeg 3.3.2 版本或将 file:// 等危险协议类型添加到黑名单等方式解决这个问题。

参考链接：<http://www.freebuf.com/vuls/138377.html>

2. 关于 Petya 勒索病毒有关情况的预警通报

北京时间 2017 年 6 月 27 日晚，据外媒消息，乌克兰等多国正在遭遇 Petya 勒索病毒袭击，政府、银行等重要系统受攻击影响。此次黑客使用的是 Petya 勒索病毒的变种 Petwarp，使用的攻击方式和 WannaCry 相同。通过对本次事件跟踪分析发现，攻击事件

中的病毒属于 Petya 勒索者的变种 Petwrap，病毒使用 MicrosoftOffice/WordPad 远程执行代码漏洞（CVE-2017-0199）通过电子邮件进行传播，感染成功后利用永恒之蓝漏洞，在内网中寻找打开 445 端口的主机进行传播。

参考链接：<http://www.freebuf.com/news/138584.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