

国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 08 月 08 日-2016 年 08 月 14 日

2016年第33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 219 个，其中高危漏洞 78 个、中危漏洞 130 个、低危漏洞 11 个。漏洞平均分为 6.36 分。本周收录的漏洞中，涉及 0day 漏洞 20 个（占 9%）。其中互联网上出现“NUUO NVRmini 2 任意代码执行漏洞、NUUO NVRmini 2 远程代码执行漏洞”等零日代码攻击漏洞，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 1568 个，与上周（1282 个）环比增长 22.3%。

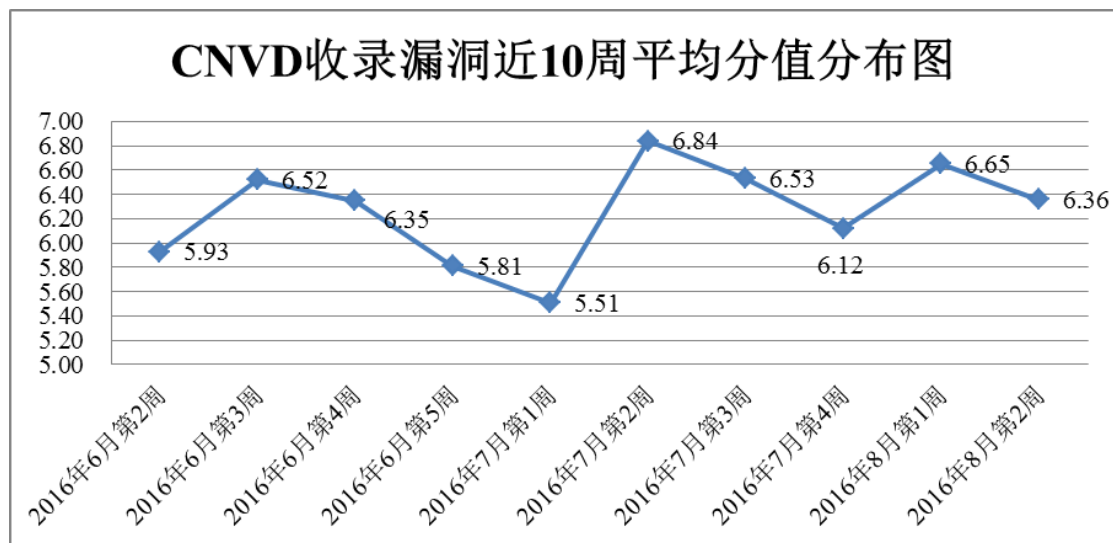


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 9 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 219 个漏洞。报送情况如表 1 所示。其中，奇虎（补天平台）、天融信、启明星辰、东软、等单位报送数量较多。补天平台、漏洞盒子及其他个人白帽子向 CNVD 提交了 1568 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）	1495	1495
安天实验室	225	0
天融信	224	0
启明星辰	181	1
东软	107	0
H3C	90	0
恒安嘉新	71	0
杭州安恒信息技术有限公司	48	0
中国电信集团系统集成有限责任公司	35	0
漏洞盒子	32	32
CNCERT 宁夏分中心	8	8
CNCERT 天津分中心	7	7
CNCERT 上海分中心	5	5
CNCERT 江西分中心	4	4
CNCERT 安徽分中心	2	2
个人	14	14
报送总计	2548	1568
录入总计	219（去重）	1568

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 219 个漏洞。其中应用程序漏洞 114 个，操作系统漏洞 68 个，网络设备漏洞 25 个，web 应用漏洞 11 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	114
操作系统漏洞	68
网络设备漏洞	25
web 应用漏洞	11
数据库漏洞	1

表 2 漏洞按影响类型统计表

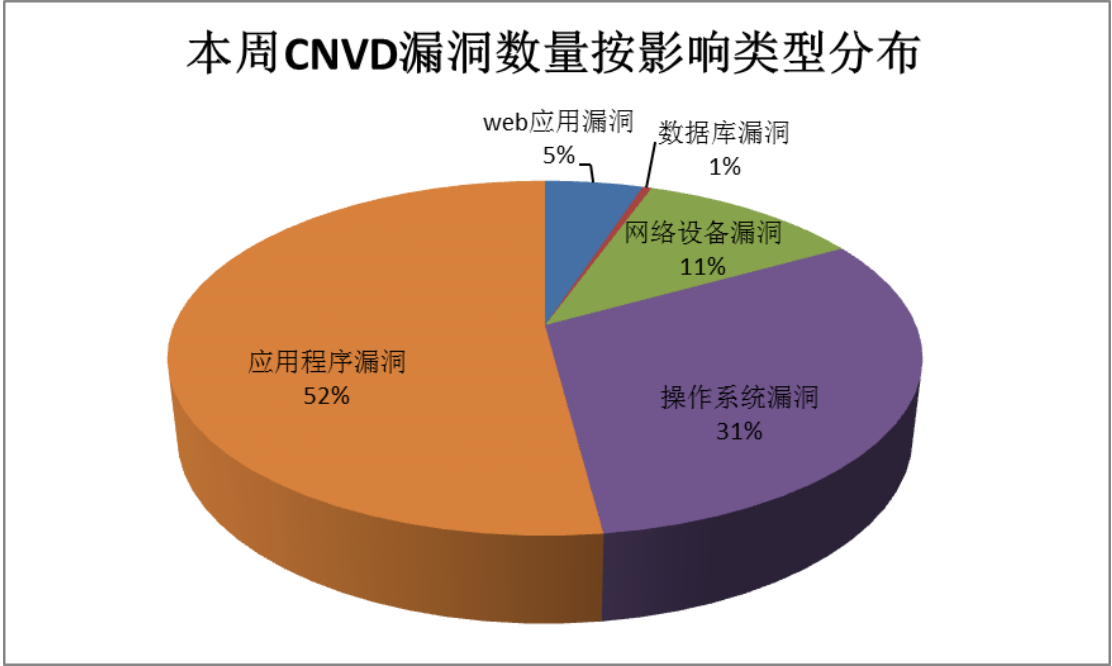


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Microsoft、Mozilla 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	Google	102	47%
2	Microsoft	28	13%
3	Mozilla	23	11%
4	Cisco	9	4%
5	Qualcomm Innovation Center, Inc	7	3%
6	IBM	5	2%
7	WordPress	5	2%
8	Adobe	4	2%
9	Wireshark	4	2%
10	其他	32	14%

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 6 个电信行业漏洞，76 个移动互联网行业漏洞（如下图所示）。其中，“Android on Nexus devices 权限提升漏洞(CNVD-2016-06288、CNVD-2016-06290、CNVD-2016-06291、CNVD-2016-06292、CNVD-2016-06293、CNVD-2016-06294)、Android on Nexus Qualcomm 组件权限获取漏洞（CNVD-2016-06224、CNVD-2016-06234、CNVD-2016-06242、CNVD-2016-06244）”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/>

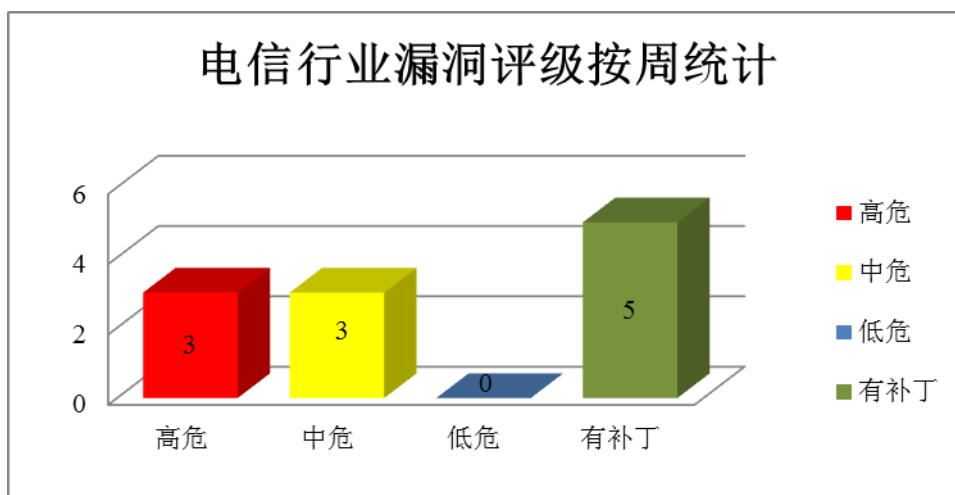


图 3 电信行业漏洞统计

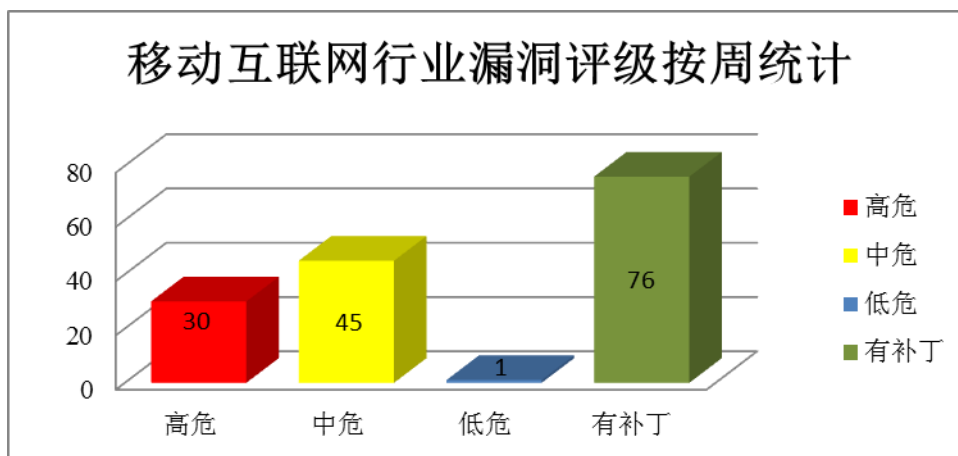


图 4 移动互联网行业漏洞统计

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、Microsoft 产品安全漏洞

8月9日，微软发布了2016年8月份的月度例行安全公告，共含9项更新，修复了Microsoft Windows、Internet Explorer、Edge、Office、Microsoft 通信平台和软件中存在的27个安全漏洞。其中，5项远程代码更新的综合评级为最高级“严重”级别。利用上述漏洞，攻击者可提升权限，远程执行任意代码。

CNVD收录的相关漏洞包括：Microsoft Win32k 权限提升漏洞（CNVD-2016-06263、CNVD-2016-06264、CNVD-2016-06265、CNVD-2016-06299）、Microsoft Office 内存破坏漏洞（CNVD-2016-06268、CNVD-2016-06269、CNVD-2016-06270、CNVD-2016-06271）等。其中，“Microsoft Office 内存破坏漏洞（CNVD-2016-06268、CNVD-2016-06269、CNVD-2016-06270、CNVD-2016-06271）”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/webinfo/show/3907>

2、Google 产品安全漏洞

Android on Nexus 5和7是美国谷歌（Google）公司和开放手持设备联盟（简称OHA）共同开发的一套运行于Nexus 5和7（智能手机）中并以Linux为基础的开源操作系统。Qualcomm是使用在其中的一个美国高通（Qualcomm）公司的设备专用的高通组件。本周，该产品被披露存在权限获取漏洞，攻击者可利用漏洞获取权限。

CNVD收录的相关漏洞包括：Android on Nexus Qualcomm 组件权限获取漏洞（CNVD-2016-06231、CNVD-2016-06233、CNVD-2016-06243、CNVD-2016-06246、CNVD-2016-06247、CNVD-2016-06248、CNVD-2016-06249、CNVD-2016-06250）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-2016-06231>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06233>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06243>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06246>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06247>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06248>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06249>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06250>

3、Mozilla 产品安全漏洞

Mozilla Firefox 是一款开源 Web 浏览器；Firefox ESR 是 Firefox 的一个延长支持版本。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞提执行任意代码、泄露敏感信息、进行跨站脚本攻击或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Firefox ESR 拒绝服务漏洞（CNVD-2016-06138）、Mozilla Firefox 和 Firefox ESR 栈缓冲区溢出漏洞、Mozilla Firefox 密码获取漏洞、Mozilla Firefox 和 Firefox ESR 内存破坏漏洞（CNVD-2016-06148）、Mozilla Firefox 和 Firefox ESR 跨站脚本漏洞、Mozilla Firefox 和 Firefox ESR 'nsDisplayList::HitTest'函数任意代码执行漏洞、Mozilla Firefox 和 Firefox ESR 信息泄露漏洞、Mozilla Firefox 和 Firefox ESR 存在未明内存破坏漏洞等。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-2016-06138>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06170>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06173>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06148>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06151>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06155>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06121>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06101>

4、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（包括 IOS T、IOS S 和 IOS XR）中的一套完全模块化、分布式的网络操作系统。Cisco RV180、RV180W、RV110W、RV130W 和 RV215W 均为思科公司路由器产品。Cisco IOS 是美国思科（Cisco）公司为其网络设备开发的操作系统。Cisco TelePresence Video Communication Server Expressway 是美国思科（Cisco）公司的一款网真视频通信服务器，Cisco Unified Communications Manager 是一款统一通信系统中的呼叫处理组件。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞遍历目录、执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco IOS XR Software 远程拒绝服务漏洞、Cisco RV180/RV180W 任意命令执行漏洞、Cisco RV180/RV180W 目录遍历漏洞、Cisco IOS 拒绝服务漏洞（CNVD-2016-06186）、多款 Cisco 产品安全绕过漏洞、多款 Cisco 产品存在任意命令执行漏洞、Cisco TelePresence Video Communication Server Expressway 命令注入漏洞、Cisco Unified Communications Manager IM and Presence Service 拒绝服务漏洞等。其中，“Cisco RV180/RV180W 任意命令执行漏洞、多款 Cisco 产品安全绕过漏洞、Cisco Unified Communications Manager IM and Presence Service 拒绝服务漏洞”的综合评级为“高危”。目前，厂商已经发布了除“Cisco RV180/RV180W 任意命令执行漏洞”以外漏洞的修补程序。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-2016-06305>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06187>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06190>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06186>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06160>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06162>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06103>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-06102>

5、NUUO NVRmini 2 任意代码执行漏洞

NUUO 提供一个稳定的和高性能的数字联网监控系统。本周，NUUO NVRmini 2 被披露存在任意代码执行漏洞。攻击者可利用该漏洞以 root 权限注入和执行任意代码。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-2016-06194>

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-2016-06093	ImageMagick 缓冲区溢出漏洞（CNVD-2016-06093）	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.imagemagick.org/
CNVD-2016-06109	Crestron AirMedia AM-100 rftest.cgi 目录遍历漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://github.com/CylanceVulnResearch/disclosures/blob/master/CLVA-2016-05-002.md
CNVD-2016-06107	Moxa SoftCMS SQL 注入漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.moxa.com/product/SoftCMS.htm
CNVD-2016-06093	ImageMagick 缓冲区溢出漏洞（CNVD-2016-06093）	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.imagemagick.org/
CNVD-2016-06109	Crestron AirMedia AM-100 rftest.cgi 目录遍历漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://github.com/CylanceVulnResearch/disclosures/blob/master/CLVA-2016-05-002.md
CNVD-2016-06107	Moxa SoftCMS SQL 注入漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www.moxa.com/product/SoftCMS.htm

CNVD-2016-06115	IBM QRadar SIEM OS 命令注入漏洞	高	用户可参考如下厂商提供的安全公告获取补丁以修复该漏洞： http://www-01.ibm.com/support/docview.wss?uid=swg21988094
CNVD-2016-06185	Qualcomm Innovation Center Android contributions for MSM 内存破坏漏洞	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： https://www.kernel.org/
CNVD-2016-06184	Qualcomm Innovation Center Android contributions for MSM 内存错误引用漏洞	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： https://www.kernel.org/
CNVD-2016-06198	WordPress SSRF 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： http://codex.wordpress.org/Version_4.5

表 4 部分重要高危漏洞列表

小结：本周，8月9日，微软发布了2016年8月份的月度例行安全公告，共含9项更新，修复了Microsoft Windows、Internet Explorer、Edge、Office、Microsoft 通信平台和软件中存在的27个安全漏洞。此外，Google、Mozilla、Cisco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，NUUO NVRmini 2被披露存在任意代码执行漏洞。攻击者可利用该漏洞以root权限注入和执行任意代码。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. 高通曝 Quadrooter 高危漏洞，影响全球9亿安卓用户

近日，Check Point 安全公司的研究人员在拉斯维加斯的DEF CON 24安全会议上对此4种新漏洞进行了披露。据悉，该4个新漏洞分别为CVE-2016-2503（发现于高通GPU驱动程序，分析见谷歌的2016年8月Android安全公告）；CVE-2016-2504（高通GPU驱动程序中，分析见谷歌的2016年7月Android安全公告）；CVE-2016-2059（高通内核模块中，4月修复，补丁状态未知）以及CVE-2016-5340（高通GPU驱动程序中，已修复，补丁状态未知）。影响全球9亿多安卓用户，通过这些漏洞，黑客可以完全控制受影响的手机。然而，修复所有设备需要相当长的一段时间，因为高通芯片的固件补丁需要由安卓OEM供应商集成到其安卓操作系统定制版本，再将其送至移动运营商处，移动运营商决定在合适的时间将其交付最终用户。修复这些漏洞的补丁要到9月份才会全面发布。

参考链接：<http://www.freebuf.com/vuls/111362.html>

2. Linux 设备 TCP 连接曝高危漏洞：只要接入网络就可能被攻击

CVE-2016-5696 漏洞主要影响的是 Linux 系统。具体说来，Linux 内核版本在 v3.6 至 v4.7 之间的系统都受到影响，也就是过去 4 年间的各类 Linux 系统受到影响。利用该漏洞在服务器和客户端的 TCP 连接中进行流量劫持攻击，服务器和客户端是不需要植入任何恶意程序的。实际上，针对该漏洞的 Linux 内核补丁已经开发完成，而且如上所述，研究人员也专门为客户端和服务端主机设备开发了相应的补丁，增加该漏洞的利用难度。

参考链接：<http://www.freebuf.com/news/111735.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