

信息安全漏洞周报

2016 年 09 月 12 日-2016 年 09 月 18 日

2016 年第 38 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 183 个，其中高危漏洞 87 个、中危漏洞 90 个、低危漏洞 6 个。漏洞平均分为 6.58。本周收录的漏洞中，涉及 0day 漏洞 49 个（占 27%）。其中互联网上出现“Oracle MySQL 远程命令执行漏洞、libupnp 堆缓冲区溢出漏洞”等零日漏洞，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 512 个，与上周（968 个）环比下降 47%。

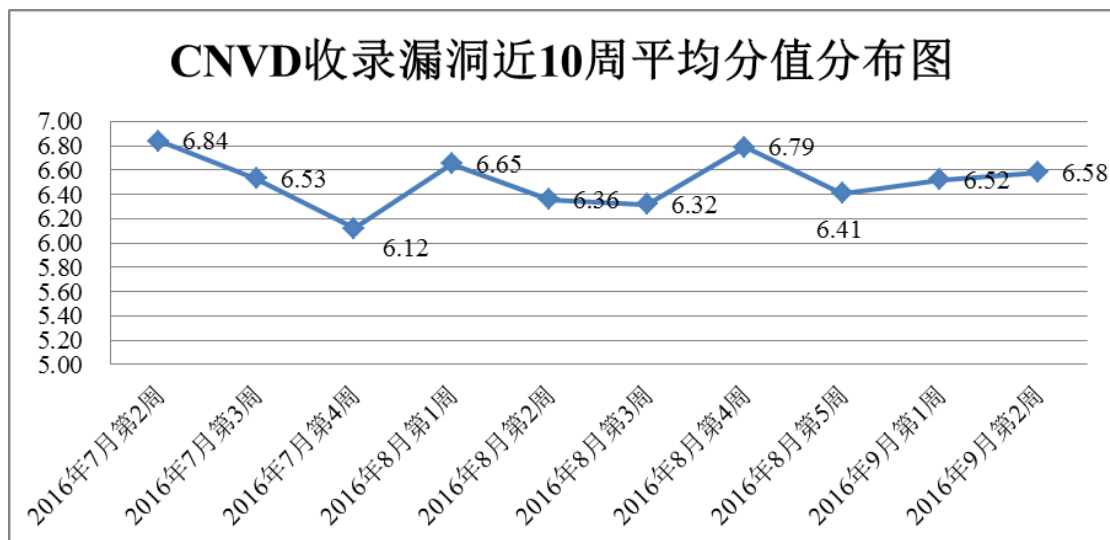


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 10 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 183 个漏洞。报送情况如表 1 所示。其中，安天实验室、恒安嘉新、启明星辰、东软等单位报送数量较多。奇虎（补天平台）、漏洞盒子、腾讯玄武实验室、上海云盾信息技术有限公司、广东电网有限责任公司电力科学研究院、广州圣辉信息技术有限公司、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、西安四叶草信息技术有限公司及其他个人白帽子向 CNVD 提交了 512 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）	438	438
安天实验室	125	0
恒安嘉新	102	0
启明星辰	93	3
东软	83	0
H3C	78	0
天融信	77	0
绿盟科技	67	0
中国电信集团系统集成有限责任公司	42	0
杭州安恒信息技术有限公司	13	13
漏洞盒子	13	13
腾讯玄武实验室	10	10
上海云盾信息技术有限公司	7	7
广东电网有限责任公司电力科学研究院	3	3
广州圣辉信息技术有限公司	3	3
中国航天科工四院软件评测中心	3	3
深圳市深信服电子科技有限公司	2	2
西安四叶草信息技术有限公司	2	2
CNCERT 福建分中心	2	2
个人	13	13

报送总计	1176	512
录入总计	183（去重）	512

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 183 个漏洞。其中应用程序漏洞 91 个，操作系统漏洞 45 个，web 应用漏洞 32 个，网络设备漏洞 13 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	91
操作系统漏洞	45
web 应用漏洞	32
网络设备漏洞	13
数据库漏洞	2

表 2 漏洞按影响类型统计表

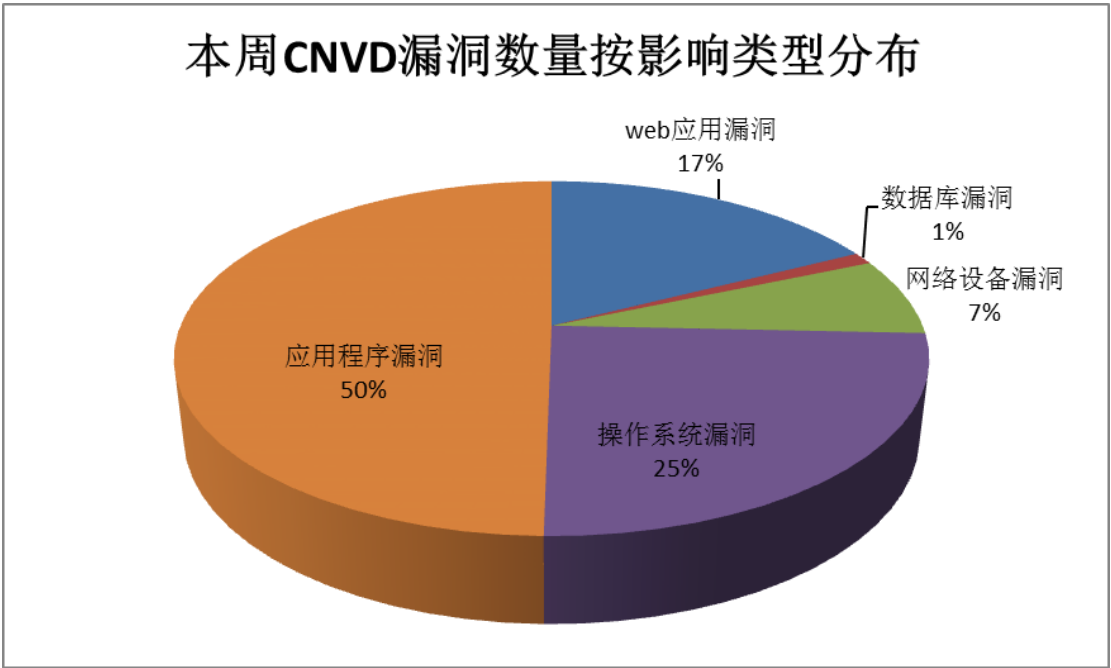


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、Microsoft、Adobe 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	37	20%
2	Microsoft	32	17%
3	Adobe	8	4%

4	Trend Micro	6	3%
5	Wireshark	6	3%
6	BINOM3 Electric Power Quality Meter	6	3%
7	Open-Xchange	4	3%
8	Cisco	4	3%
9	ASUS	3	2%
10	其他	77	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 个电信行业漏洞，36 个移动互联网行业漏洞（如下图所示）。其中，“Huawei WS331a 跨站请求伪造漏洞、Google Android Mediaserver 权限提升漏洞（CNVD-2016-07547、CNVD-2016-07462、CNVD-2016-07463）、Android 权限提升漏洞（CNVD-2016-07428）、Android LibUtils 任意代码执行漏洞、Android 权限提升漏洞（CNVD-2016-07422）、Android MediaMuxer 任意代码执行漏洞、Google Android 远程权限提升漏洞（CNVD-2016-07420）、Google Nexus NVIDIA kernel 权限提升漏洞”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/>

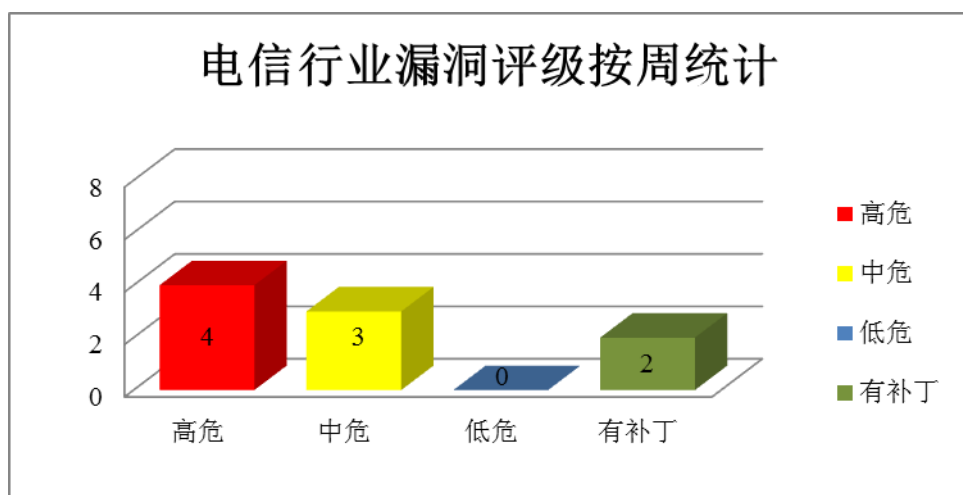


图 3 电信行业漏洞统计

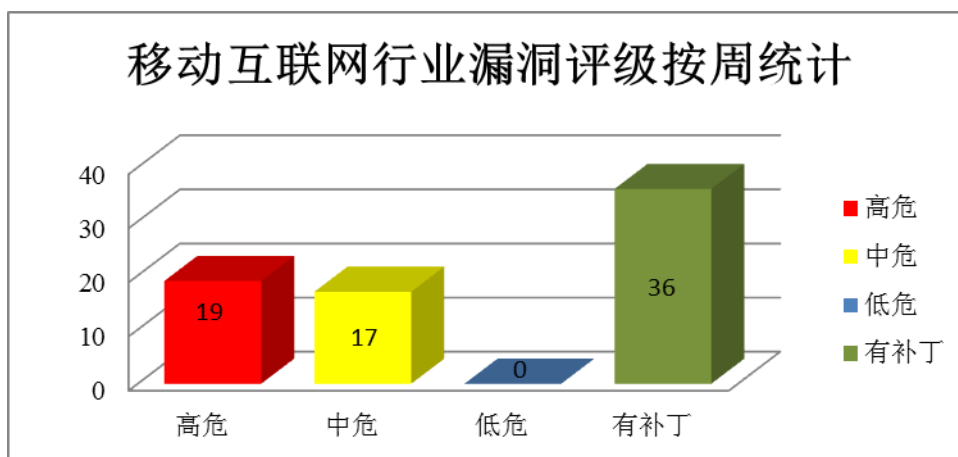


图 4 移动互联网行业漏洞统计

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

9 月 13 日，微软发布了 2016 年 9 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、Office Services 和 Web Apps 和 Exchange 中存在的 50 个安全漏洞。其中，7 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 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CNVD 收录的相关漏洞包括：Microsoft Office 内存破坏漏洞（CNVD-2016-07580、CNVD-2016-07579、CNVD-2016-07578、CNVD-2016-07577、CNVD-2016-07576、CNVD-2016-07575、CNVD-2016-07574、CNVD-2016-07573）等。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-2016-07580>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07579>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07578>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07577>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07576>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07575>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07574>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07573>

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（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。Qualcomm Sound Driver 是使用在其中的一个美

国高通（Qualcomm）公司开发的声音驱动程序。Qualcomm Camera Driver 是摄像头驱动程序。Qualcomm power driver 是电源连接驱动组件。Qualcomm radio interface layer 是其中的一个 Android 电话服务和无线电硬件之间的无线接口层（RIL）。Qualcomm IPA driver 是其中的一个网络加速器组件。本周，上述产品被披露存权限提升漏洞，攻击者可利用该漏洞获取提升的权限。

CNVD 收录的相关漏洞包括：Google Android Qualcomm 无线接口层权限提升漏洞、Google Android Qualcomm 声音驱动程序权限提升漏洞、Google Android Qualcomm 摄像头驱动权限提升漏洞、Google Android Qualcomm power driver 权限提升漏洞、Google Android Qualcomm IPA 驱动程序权限提升漏洞、Google Android Mediaserver 权限提升漏洞（CNVD-2016-07547、CNVD-2016-07463、CNVD-2016-07462）等。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-2016-07562>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07560>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07561>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07558>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07559>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07547>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07463>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07462>

3、Adobe 产品安全漏洞

Adobe Digital Editions 是一款由 Adobe 公司开发的电子书阅读管理工具。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用此漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Digital Editions 远程代码执行漏洞（CNVD-2016-07619、CNVD-2016-07527、CNVD-2016-07528、CNVD-2016-07529、CNVD-2016-07530、CNVD-2016-07531、CNVD-2016-07532）、Adobe Digital Editions 远程代码执行漏洞等。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-2016-07619>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07527>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07528>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07529>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07530>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07531>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07532>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07533>

4、Trend Micro 产品安全漏洞

Trend Micro Smart Protection Server 是一个端点保护套件。Trend Micro InterScan Messaging Security 是一种混合型的 SaaS 电子邮件安全解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、获取提升的权限或进行跨站脚本攻击等。

CNVD 收录的相关漏洞包括：Trend Micro Smart Protection Server 目录遍历漏洞、Trend Micro Smart Protection Server 远程代码执行漏洞、Trend Micro Smart Protection Server 权限提升漏洞、Trend Micro InterScan Messaging Security 跨站脚本漏洞、Trend Micro InterScan Messaging Security 开放重定向漏洞、Trend Micro InterScan Messaging Security 存在多个漏洞。其中，“Trend Micro Smart Protection Server 远程代码执行漏洞、Trend Micro Smart Protection Server 权限提升漏洞”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-2016-07452>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07450>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07451>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07449>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07448>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-07447>

5、Oracle MySQL 远程命令执行漏洞

Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。本周，Oracle MySQL 被披露存在远程命令执行漏洞。攻击者可利用该漏洞以 root 权限执行任意代码。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-2016-07549>

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-2016-07416	libunp 堆缓冲区溢出漏洞	高	暂无
CNVD-2016-07424	Huawei WS331a 跨站请求伪造漏洞	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.huawei.com/en/psirt/security-advisories/huawei-sa-20160907-01-ws331a-en

CNVD-2016-07480	Linux Kernel 远程缓冲区溢出漏洞	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.linux.org/
CNVD-2016-07478	TYPO3 Speaking URLs for TYPO3 拒绝服务漏洞	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://typo3.org/teams/security/security-bulletins/typo3-extensions/typo3-ext-sa-2016-021/
CNVD-2016-07556	AlienVault Unified Security Management 远程命令执行漏洞	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.alienvault.com/forums/discussion/7110/
CNVD-2016-07564	Red Hat JBoss Enterprise Application Platform HTTP 头注入漏洞	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://bugzilla.redhat.com/show_bug.cgi?id=1344321
CNVD-2016-07567	Blue Coat K9 Web Protection 远程命令执行漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，详情请关注厂商主页： https://www.bluecoat.com/
CNVD-2016-07570	AVer Information EH6108H+ hybrid DVR VU 硬编码凭据漏洞	高	暂无
CNVD-2016-07571	AVer Information EH6108H+ hybrid DVR VU 认证绕过漏洞	高	暂无
CNVD-2016-07618	HPE Performance Center 远程安全绕过漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c05269356

表 4 部分重要高危漏洞列表

小结：9月13日，微软发布了2016年9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、Office Services 和 Web Apps 和 Exchange 中存在的50个安全漏洞。此外，Google、Adobe、Trend Micro 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提升的权限、执行任意代码或进行跨站脚本攻击等。另外，Oracle MySQL 被披露存在远程命令执行漏洞。攻击者可利用该漏洞以root权限执行任意代码。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. FFMpeg 3.1.3 修复来自支付宝 unLimit Security Team 的高危漏洞

FFMpeg 是一套可以用来记录、转换数字音频、视频，并能将其转化为流的开源计算机程序，包括了目前领先的音/视频编码库 libavcodec。据悉很多软件及系统中，包括现在很多主流的移动端 APP 采用了 FFMpeg，意味着大量的软件及系统都被暴露于网络攻击之下。支付宝移动安全团队 unLimitSecurity Team 的安全研究员超六，发现 ffmpeg 在解码 exr 文件时存在一个堆溢出漏洞，CVE 编号为 CVE-2016-6920。该漏洞存在于解析 exr 图片文件时，程序对输入参数校验不严，可能导致任意地址写，并且写入数据部分可控。此漏洞在一定条件下能导致任意地址写。ffmpeg3.1.3 中已修复该漏洞，建议使用 ffmpeg 处理 exr 文件的软件及系统尽快升级至最新版。

参考链接：<http://www.freebuf.com/vuls/114484.html>

2. 漏洞预警：MySQL 代码执行 0-day 漏洞 可本地提权

来自波兰的安全研究人员 Dawid Golunski 刚刚发现了两个 MySQL 的 0-day 漏洞，影响到所有版本分支、默认配置的 MySQL 服务器（5.7、5.6 和 5.5），包括最新版本。攻击者可以远程和本地利用漏洞。攻击者成功利用漏洞后，可以 ROOT 权限执行代码，完全控制 MySQL 数据库。攻击者仅需有 FILE 权限即可实现 ROOT 提权，进而控制服务器。MariaDB 和 PerconaDB 已经发布补丁修复漏洞，Oracle 方面则需要等到下一波推送的 10 月关键补丁更新，具体时间是 10 月 18 日。

参考链接：<http://www.freebuf.com/vuls/114408.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