

信息安全漏洞周报

2016 年 12 月 05 日-2016 年 12 月 11 日

2016 年第 50 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 175 个，其中高危漏洞 62 个、中危漏洞 103 个、低危漏洞 10 个。漏洞平均分为 5.99。本周收录的漏洞中，涉及 0day 漏洞 46 个（占 26%）。其中互联网上出现“Wordpress 插件 Single Personal Message SQL 注入漏洞、F3 designs 网站 SQL 注入漏洞”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 1054 个，与上周（771 个）环比增长 37%。

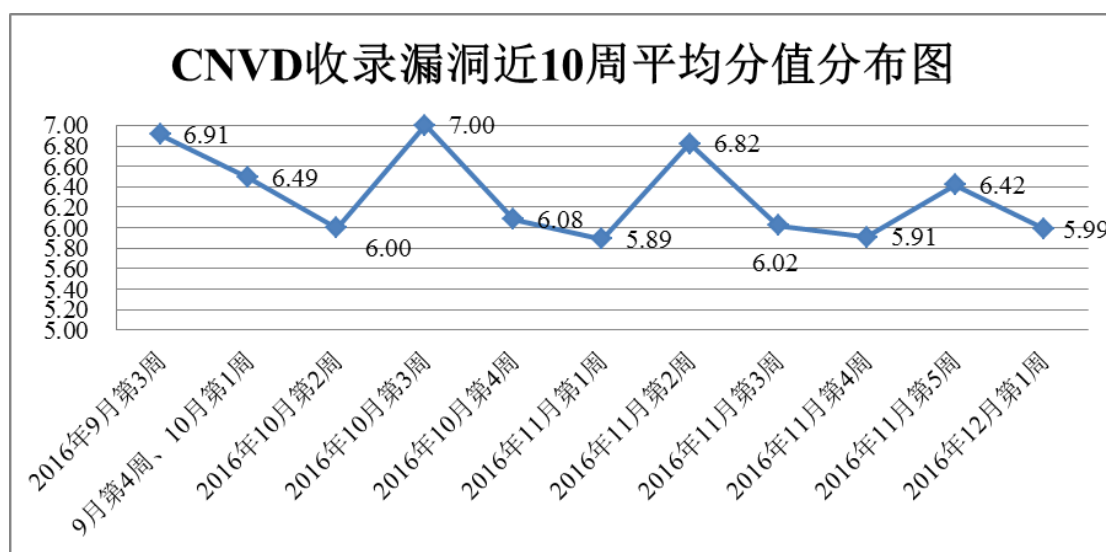


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 12 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 175 个漏洞。报送情况如表 1 所示。其中，安天实验室、蓝盾信息安全技术股份有限公司、天融信、恒安嘉新等单位报送数量较多。360 网神、漏洞盒子、广西鑫瀚科技有限公司、

南京铨迅信息技术股份有限公司、江西安服信息产业有限公司、北京安码科技有限公司及其他个人白帽子向 CNVD 提交了 1054 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	885	885
安天实验室	213	0
蓝盾信息安全技术股份有限公司	204	0
天融信	172	0
恒安嘉新	100	0
启明星辰	81	13
绿盟科技	73	0
H3C	67	0
华为技术有限公司	53	0
中国电信集团系统集成有限责任公司	31	0
北京数字观星科技有限公司	5	0
南京铨迅信息技术股份有限公司	2	2
漏洞盒子	37	37
广西鑫瀚科技有限公司	24	24
江西安服信息产业有限公司	1	1
北京安码科技有限公司	1	1
CNCERT 宁夏分中心	4	4
CNCERT 江西分中心	3	3
CNCERT 新疆分中心	1	1
CNCERT 上海分中心	1	1
个人	82	82

报送总计	2040	1054
录入总计	175（去重）	1054

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 175 个漏洞。其中应用程序漏洞 108 个，web 应用漏洞 27 个，网络设备漏洞 23 个，操作系统漏洞 13 个，安全产品漏洞 3 个，数据库漏洞 1 条。

漏洞影响对象类型	漏洞数量
应用程序漏洞	108
web 应用漏洞	27
网络设备漏洞	23
操作系统漏洞	13
安全产品漏洞	3
数据库漏洞	1

表 2 漏洞按影响类型统计表

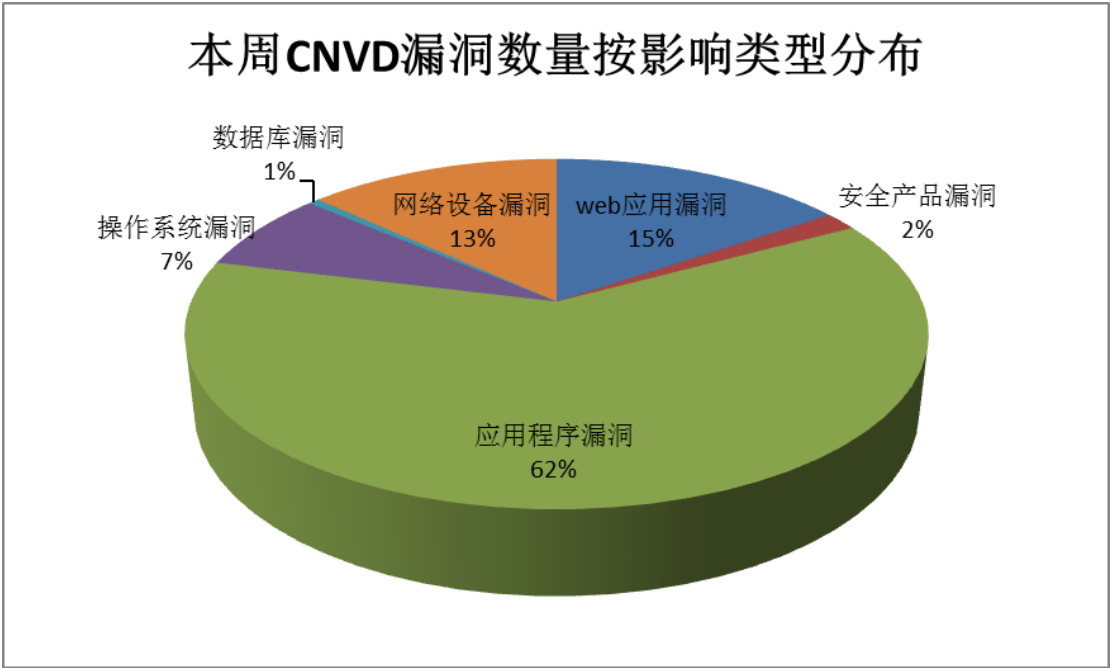


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Mozilla、IBM、JasPer 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	IBM	22	13%
2	phpMyAdmin	15	9%

3	Linux	8	5%
4	Moxa	8	5%
5	WordPress	7	4%
6	BlueZ	6	3%
7	Microsoft	5	3%
8	Apache	5	3%
9	Drupal	5	3%
10	其他	94	52%

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 2 个电信行业漏洞，4 个移动互联网行业漏洞，5 个工控系统行业漏洞（如下图所示）。其中，“Android GPS 组件拒绝服务漏洞（CNVD-2016-12023）、多个 Mitsubishi Electric MELSEC-Q 系列产品存在安全绕过漏洞、多个 Mitsubishi Electric MELSEC-Q 系列产品存在绝服务漏洞、HP Network Automation 远程代码执行漏洞”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/>

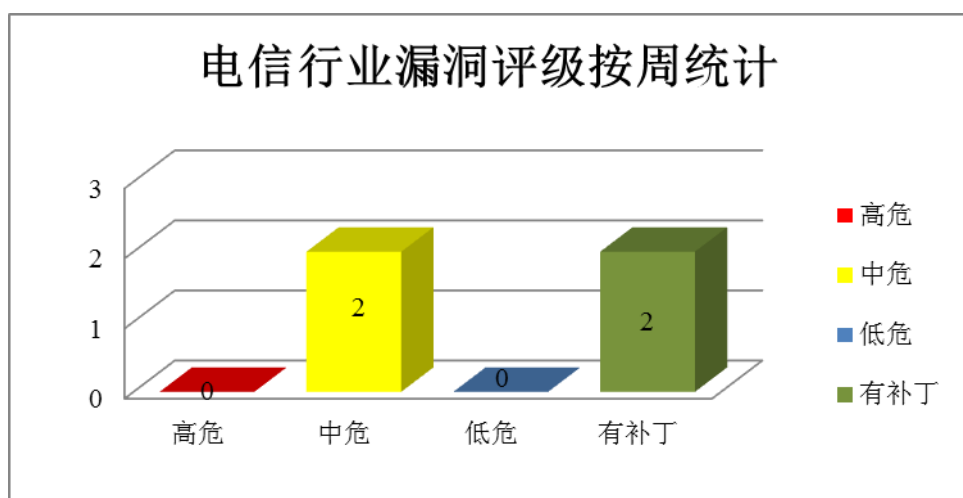


图 3 电信行业漏洞统计

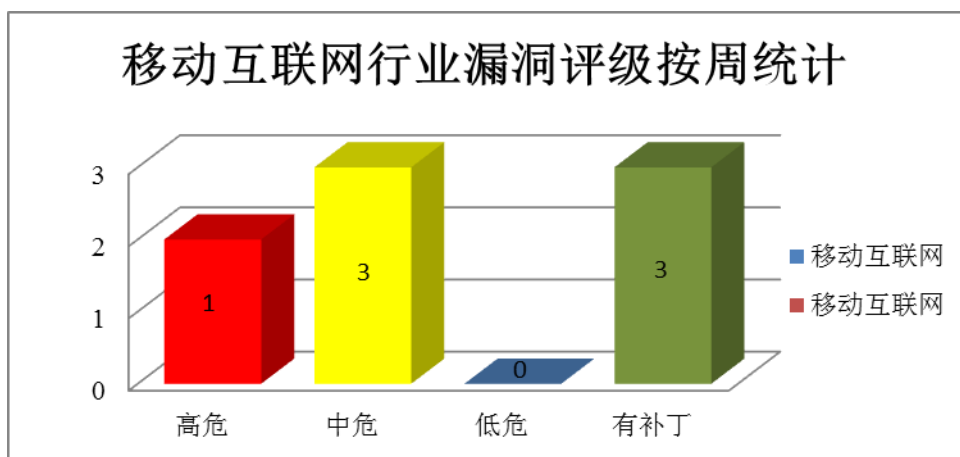


图 4 移动互联网行业漏洞统计

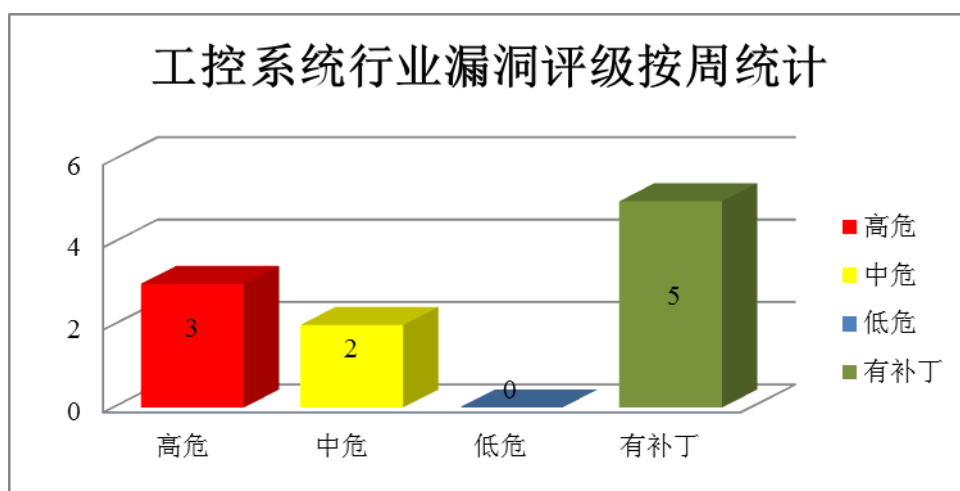


图 5 工控系统行业漏洞统计

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、Moxa 产品安全漏洞

MOXA Nport 是一款串口通讯服务器。本周，该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、进行跨站脚本攻击或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Moxa NPort 拒绝服务漏洞、Moxa NPort 明文存储漏洞、Moxa NPort 身份验证漏洞、Moxa NPort 跨站请求伪造漏洞、Moxa NPort 跨站脚本漏洞、Moxa NPort 缓冲区溢出漏洞、Moxa NPort 访问控制漏洞、Moxa NPort 凭证管理漏洞。除“Moxa NPort 明文存储漏洞、Moxa NPort 跨站脚本漏洞”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-2016-11878>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11879>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11880>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11881>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11882>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11883>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11884>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11885>

2、ImageMagick 产品安全漏洞

ImageMagick 是美国 ImageMagick Studio 公司的一套开源的图象处理软件。本周，该产品被披露存在远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：ImageMagick 存在 TIFF 文件远程代码执行漏洞。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/webinfo/show/4004>

3、IBM 产品安全漏洞

IBM BigFix Remote Control 是美国 IBM 公司的一套远程控制系统。IBM FileNet 是一套企业内容管理平台。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞泄露敏感信息、上传任意文件或执行任意 SQL 命令等。

CNVD 收录的相关漏洞包括：IBM FileNet Workplace XT 任意文件上传漏洞、IBM BigFix Remote Control SQL 注入漏洞、IBM BigFix Remote Control 信息泄露漏洞（CNVD-2016-11868、CNVD-2016-11859、CNVD-2016-11860、CNVD-2016-11861）、IBM BigFix Remote Control 目录遍历漏洞、IBM BigFix Remote Control 本地信息泄露漏洞等。除“IBM BigFix Remote Control 信息泄露漏洞（CNVD-2016-11860、CNVD-2016-11861）、IBM BigFix Remote Control 本地信息泄露漏洞”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-2016-11911>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11867>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11868>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11859>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11861>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11860>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11848>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11901>

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，该

产品被披露存在多个漏洞，攻击者可利用漏泄露敏感信息、提升本地权限或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括:Linux Kernel 本地权限提升漏洞(CNVD-2016-11972)、Linux kernel 'net/core/sock.c'存在多个内存破坏漏洞、Linux kernel 'sound/core/pcm_lib.c'内存错误引用漏洞、Linux Kernel 本地拒绝服务漏洞 (CNVD-2016-12027)、Linux kernel 'lapic.c'越边界内存访问漏洞、Linux Kernel 'kvm/emulate.c'本地信息泄露漏洞、Linux kernel 越界读写入漏洞、Linux kernel 拒绝服务漏洞 (CNVD-2016-11849) 等。其中，“Linux Kernel 本地权限提升漏洞 (CNVD-2016-11972)”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-2016-11972>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12024>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12026>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12027>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12025>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11947>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-12055>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-11849>

5、Wordpress 插件 Single Personal Message SQL 注入漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台。本周，Wordpress 被披露存在 SQL 注入漏洞。攻击者可利用该漏控制应用程序，访问或修改数据，或利用底层数据库中潜在的漏洞。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-2016-12076>

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-2016-11831	Advantech SUSIAccess Server 信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.advantech.com
CNVD-2016-11829	Advantech SUSIAccess Server 本地权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.advantech.com
CNVD-2016-11832	多个 Mitsubishi Electric MELSEC-Q 系列产品存在绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.mehvac.com/en/
CNVD-201	Advantech SUSIAccess Server 目	高	厂商已发布了漏洞修复程序，请及

6-11830	录遍历漏洞		时关注更新： http://www.advantech.com
CNVD-2016-11833	多个 Mitsubishi Electric MELSEC-Q 系列产品存在安全绕过漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.mehvac.com/en/
CNVD-2016-11841	Mozilla Firefox 远程代码执行漏洞	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://www.mozilla.org/en-US/security/advisories/mfsa2016-92/
CNVD-2016-11915	Apple iCloud Setup 远程代码执行漏洞	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://support.apple.com/en-us/HT207273
CNVD-2016-11916	Red Hat CloudForms Management Engine 远程代码执行漏洞（CNVD-2016-11916）	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://rhn.redhat.com/errata/RHSA-2016-2839.html
CNVD-2016-12022	Silicon Graphics LibTIFF 整数溢出漏洞	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.libtiff.org
CNVD-2016-12036	Apache HTTP Server 拒绝服务漏洞（CNVD-2016-12036）	高	厂商已提供漏洞修补方案，请关注厂商主页及时更新： http://httpd.apache.org/

表 4 部分重要高危漏洞列表

小结：本周，Moxa 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、进行跨站脚本攻击或发起拒绝服务攻击等此外，ImageMagick、IBM、Linux 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、执行任意代码、提升权限或发起拒绝服务攻击等。另外，WordPress 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞执行任意 SQL 命令。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. 京东 2013 年的漏洞导致千万条账户数据泄露

昨天晚上，来自网络媒体一本财经的消息，12GB 京东账户数据在暗网流通，数据多达数千万条。据说本次泄露的账户数据包括了用户名、密码、邮箱地址、QQ 号、电话号码、身份证等消息。京东今天已经正式给出回应，确认这部分数据泄露是缘于 2013 年的 Struts 2 安全漏洞，并表示京东很早就已经修复了此漏洞，而且当时已经提示存在风险的账户进行安全升级。

参考链接: <http://www.freebuf.com/news/122524.html>

2. Linux 内核竞争条件漏洞, 可致本地提权

Seclists.org 最新披露了 Linux 的竞争条件漏洞, 漏洞编号为 CVE-2016-8655。此漏洞可用于从低权限进程中执行内核代码。Philip Pettersson 在 Linux (net/packet/af_packet.c) 发现条件竞争漏洞, 此漏洞可用于从未授权进程中执行内核代码。攻击者只需要本地低权限, 就能利用该漏洞致拒绝服务 (系统崩溃) 或者以管理员权限执行任意代码。新版 Ubuntu 内核已经放出, 用户升级至新版 Ubuntu 即可解决问题。

参考链接: <http://www.freebuf.com/vuls/122152.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