国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 01 月 09 日-2017 年 01 月 15 日 **2017 年第 3 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 211 个，其中高危漏洞 92 个、中危漏洞 113 个、低危漏洞 6 个。漏洞平均分值为 6.68。本周收录的漏洞中，涉及 0day 漏洞 71 个（占 34%）。其中互联网上出现“Internet Download Accelerator 缓冲区溢出漏洞、Joomla!组件 com_remository 文件上传漏洞”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 549 个，与上周（511 个）环比增长 7%。

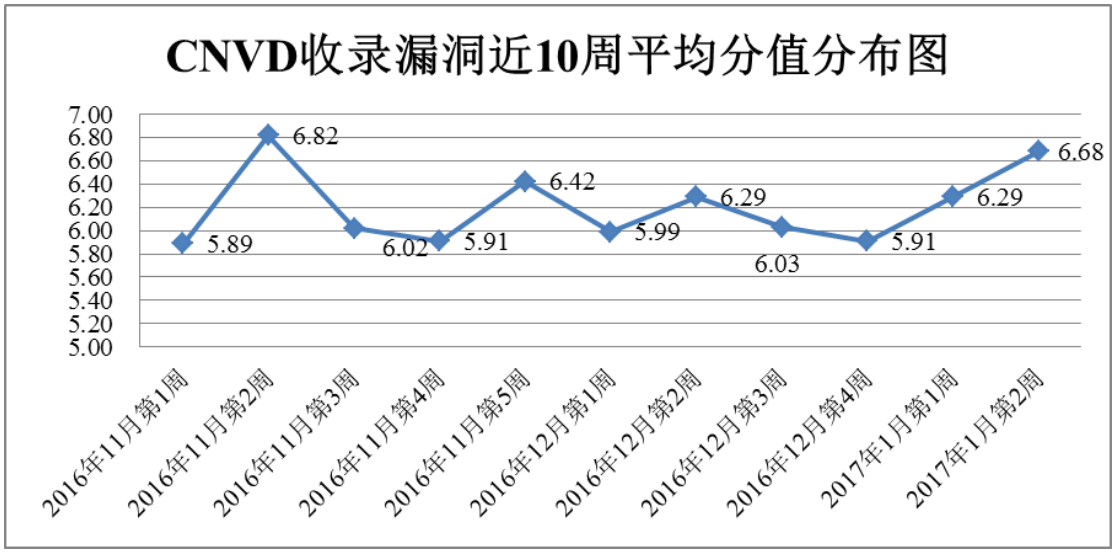

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 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 211 个漏洞。报送情况如表 1 所示。其中，安天实验室、启明星辰、天融信、华为技术有限公司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、江苏省信息

安全测评中心、新疆天山智汇信息科技有限公司、军工保密资格审查认证中心、广州神月信息安全技术有限公司、北京安码科技有限公司及其他个人白帽子向 CNVD 提交了 549 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	430	430
安天实验室	125	0
启明星辰	118	10
天融信	104	0
华为技术有限公司	90	0
H3C	88	0
东软	76	0
绿盟科技	54	0
蓝盾信息安全技术股份有限公司	54	0
恒安嘉新	24	0
中国电信集团系统集成有限责任公司	21	0
北京数字观星科技有限公司	10	0
漏洞盒子	60	60
广西鑫瀚科技有限公司	11	11
江苏省信息安全测评中心	2	2
新疆天山智汇信息科技有限公司	1	1
军工保密资格审查认证中心	1	1
广州神月信息安全技术有限公司	1	1
北京安码科技有限公司	1	1
CNCERT 湖南分中心	4	4

CNCERT 宁夏分中心	3	3
CNCERT 江西分中心	2	2
CNCERT 广东分中心	1	1
CNCERT 海南分中心	1	1
个人	21	21
报送总计	1303	549
录入总计	211（去重）	549

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 101 个漏洞。其中应用程序漏洞 112 个， web 应用漏洞 60 个，操作系统漏洞 27 个，网络设备漏洞 10 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	112
web 应用漏洞	60
操作系统漏洞	27
网络设备漏洞	10
安全产品漏洞	2

表 2 漏洞按影响类型统计表

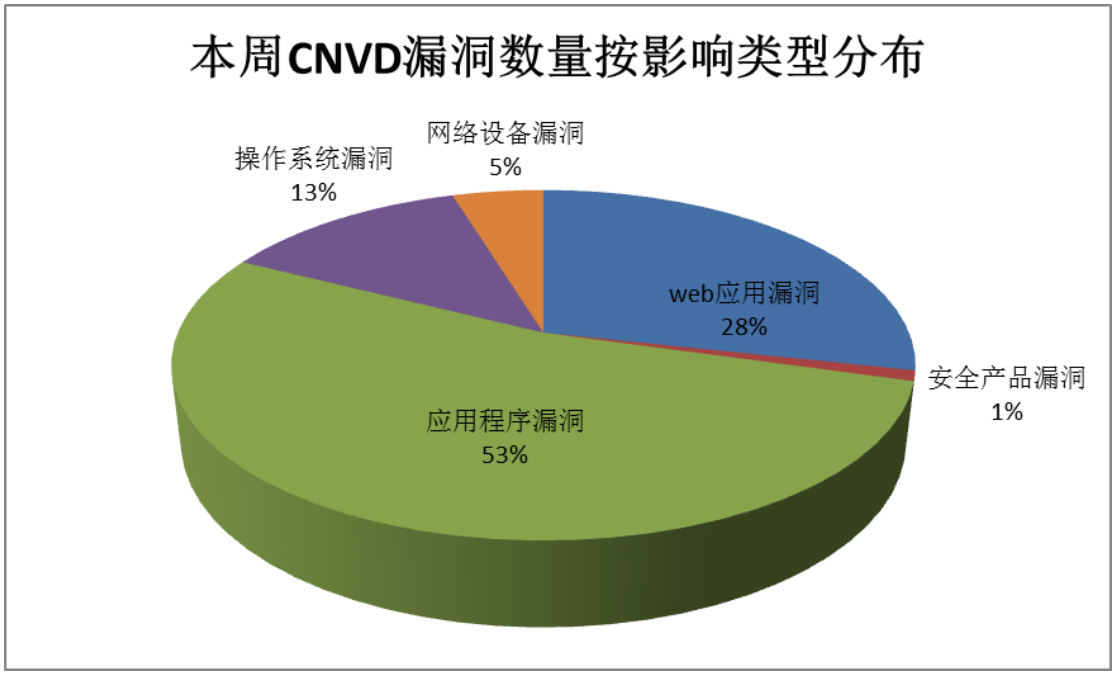

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 WordPress、Adobe、Google 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	WordPress	47	23%
2	Adobe	41	19%
3	Google	29	14%
4	IBM	15	7%
5	ImageMagick	7	3%
6	Irssi	4	2%
7	ISC	4	2%
8	EMC	3	1%
9	Microsoft	3	1%
10	其他	58	28%

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 1 个电信行业漏洞，29 个移动互联网行业漏洞,3 个工控系统行业漏洞（如下图所示）。其中，“Google Android Framesequence Library 远程代码执行漏洞（CNVD-2017-00329）、Google Android Synaptics 权限提升漏洞、Google Android Synaptics Touchscreen Driver 特权提升漏洞、Google Android One Qualcomm Radio Driver 权限提升漏洞、多个 Google Device 权限提升漏洞、Google Nexus Qualcomm Wi-Fi Driver 特权提升漏洞、多个 Google Devices 权限提升漏洞、多个 Google Devices Qualcomm Sound Driver 权限提升漏洞、Google Android 远程代码执行漏洞、Google Android NVIDIA GPU Driver 特权提升漏洞、Google Nexus Qualcomm Wi-Fi Driver 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/

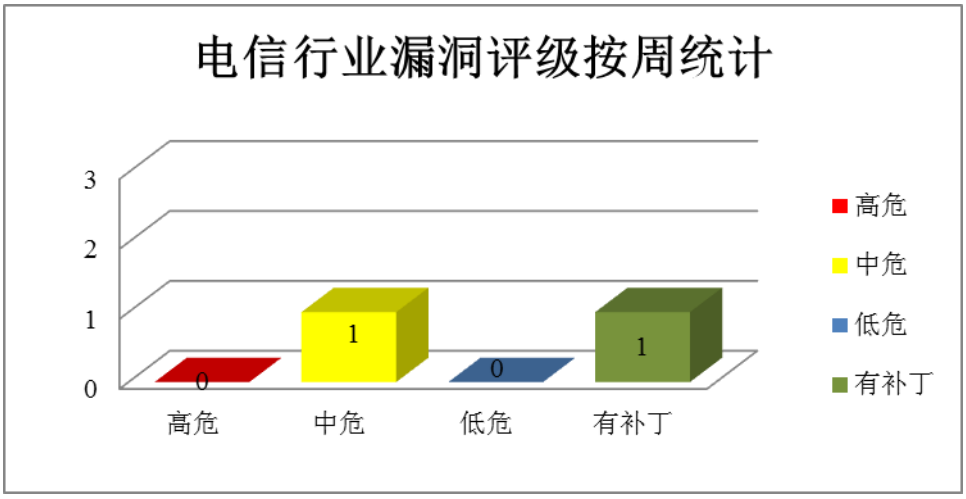

图 3 电信行业漏洞统计

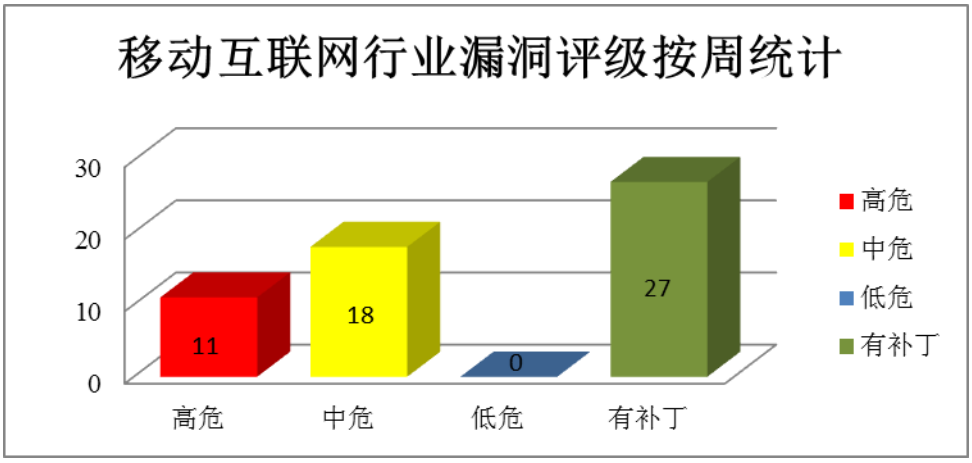

图 4 移动互联网行业漏洞统计

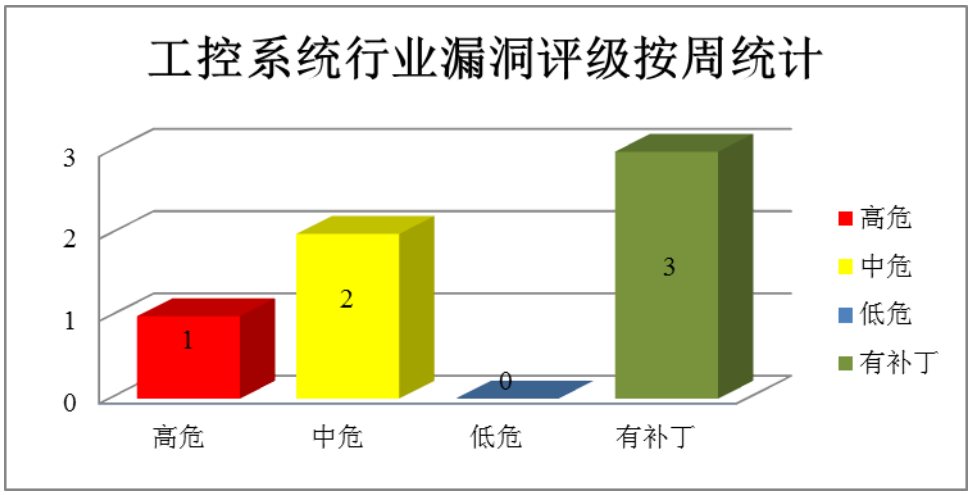

图 5 工控系统行业漏洞统计

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、Microsoft 产品安全漏洞

1 月 10 日，微软发布了 2017 年 1 月份的月度例行安全公告，共含 4 项更新，修复了 MicrosoftWindows、Edge、Office、Office Services、Web Apps 和 Adobe Flash Player 中存在的 4 个安全漏洞。其中，1 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 Edge 远程权限提升漏洞、Microsoft Office 内存破坏漏洞（CNVD-2017-00428）、Microsoft Windows LSASS 拒绝服务漏洞。除“Microsoft Edge 远程权限提升漏洞”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/webinfo/show/4031

2、ISC 产品安全漏洞

BIND 是一套开源的用于实现 DNS 协议的软件。本周，该产品被披露存在拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击，对互联网上广泛应用 BIND 系统解析软件的域名服务器构成安全运行风险。

CNVD 收录的相关漏洞包括：ISC BIND 9 db.c 断言失败拒绝服务漏洞、ISC BIND 9 DNSSEC 断言失败拒绝服务漏洞、ISC BIND 9 DS 响应断言失败拒绝服务漏洞、ISC BIND 9 RTYPE ANY 断言失败拒绝服务漏洞。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/flaw/show/CNVD-2017-00382
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00383
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00384
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00385

3、Adobe 产品安全漏洞

Adobe Acrobat 和 Reader 是美国 Adobe 公司开发的一款可以用便携式文档格式出版所有的文档的编辑软件。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 内存破坏漏洞（CNVD-2017-00399、CNVD-2017-00412、CNVD-2017-00415、CNVD-2017-00416、CNVD-2017-00417、CNVD-2017-00418、CNVD-2017-00419、CNVD-2017-00420）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-2017-00399
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00412
http://www.cnvd.org.cn/flaw/show/CNVD-2017-00415

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00416

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00417

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00418

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00419

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00420

4、Google 产品安全漏洞

Google Pixel C 等都是美国谷歌（Google）公司的智能设备。Android on Nexus 5X 等是一套运行于 Nexus 5X 等以 Linux 为基础的开源操作系统。Google Android One 是一款智能手机。Google Nexus 是搭载原装 Android 系统的高端手机系列。本周，上述产品被披露存在权限提升漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括： Google Pixel Binder 权限提升漏洞、Google Android Synaptics 权限提升漏洞、Google Android One Qualcomm Radio Driver 权限提升漏洞、多个 Google Device 权限提升漏洞、Google Nexus Qualcomm Wi-Fi Driver 特权提升漏洞、多个 Google Devices 权限提升漏洞、多个 Google Devices Qualcomm Sound Driver 权限提升漏洞、Google Nexus Qualcomm Wi-Fi Driver 权限提升漏洞等。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-2017-00342

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00341

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00332

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00334

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00335

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00337

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00339

http://www.cnvd.org.cn/flaw/show/CNVD-2017-00185

5、Joomla!组件 com_remository 文件上传漏洞

Joomla!是一款开放源码的内容管理系统(CMS)。本周，Joomla!被披露存在文件上传漏洞。攻击者可以利用该漏洞上传恶意文件到服务器从而获得服务器权限。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-2017-00253

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-2017-00187	Nagios 不完全修复本地权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			http://seclists.org/oss-sec/2016/q4/783
CNVD-2017-00314	Irssi 内存破坏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://seclists.org/oss-sec/2016/q1/610
CNVD-2017-00313	Irssi 内存破坏漏洞（CNVD-2017-00313）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://seclists.org/oss-sec/2016/q1/610
CNVD-2017-00312	Irssi 内存破坏漏洞（CNVD-2017-00312）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://seclists.org/oss-sec/2016/q1/610
CNVD-2017-00311	Irssi 内存破坏漏洞（CNVD-2017-00311）	高	厂商已发布了漏洞修复程序，请及时关注更新：http://seclists.org/oss-sec/2016/q1/610
CNVD-2017-00323	IBM UrbanCode Deploy 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-01.ibm.com/support/docview.wss?uid=swg2C1000238
CNVD-2017-00344	IBM BigFix Platform 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：http://www-01.ibm.com/support/docview.wss?uid=swg21996375
CNVD-2017-00402	Game Music Emulators 内存破坏漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://bitbucket.org/mpyne/game-music-emu/wiki/Home
CNVD-2017-00403	Game Music Emulators 内存破坏漏洞（CNVD-2017-00403）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://bitbucket.org/mpyne/game-music-emu/wiki/Home
CNVD-2017-00404	Game Music Emulators 内存破坏漏洞（CNVD-2017-00404）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://bitbucket.org/mpyne/game-music-emu/wiki/Home

表 4 部分重要高危漏洞列表

小结：1 月 10 日，微软发布了 2017 年 1 月份的月度例行安全公告，共含 4 项更新，修复了 MicrosoftWindows、Edge、Office、Office Services、Web Apps 和 Adobe Flash Player 中存在的 4 个安全漏洞。攻击者可提升权限，远程执行任意代码。此外，ISC、Adobe、Google 等多款产品被披露存在权限提升和拒绝服务漏洞，攻击者利用漏洞可执行任意代码或发起拒绝服务攻击。另外，Joomla!被披露存在文件上传漏洞。攻击者可以利用该漏洞上传恶意文件到服务器从而获得服务器权限。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. 支付宝曝“致命”漏洞，他人能改你的密码

网上曝光支付宝“熟人可以修改登录密码”的“漏洞”。据说“陌生人有 1/5 的机会登录你的支付宝，而熟人甚至 100%可以登录你的支付宝”，而且登录方式并没有什么技术含量。针对此事各个社区已经讨论炸锅，毕竟人们对支付宝的依赖非其他普通应用可比。即便这个所谓的“漏洞”如此粗糙，却的确存在危害性——支付宝修改密码的业务流程还是需要优化。

参考链接：http://www.freebuf.com/news/124847.html

2. Github 企业版程序 SQL 注入漏洞

GitHub 企业版软件是专供公司团体用来部署在内网进行开发服务的商业性应用程序。Github 企业版采用标准 OVF 格式集成，以虚拟机（VM）镜像方式发布，可以在 enterprise.github.com 网站注册下载 45 天试用版本，并把其部署在任何虚拟机环境中。这个 SQL 注入漏洞存在于 GitHub 企业版程序的 PreReceiveHookTarget 模块中，其根本原因在于/data/github/current/app/model/pre_receive_hook_target.rb 文件的第 45 行，攻击者可以控制 order 方法的参数实现恶意代码注入。

参考链接：http://www.freebuf.com/vuls/124864.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