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 22 日-2016 年 08 月 28 日　　2016 年第 35 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**高**。

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 343 个，其中高危漏洞 203 个、中危漏洞 131 个、低危漏洞 9 个。漏洞平均分值为 6.79 分。本周收录的漏洞中，涉及 0day 漏洞 183 个（占 53%）。本周，境外黑客组织“方程式组织”被泄露的涉及国内外多款防火墙漏洞以及苹果 iOS 的三个高危漏洞对互联网用户安全防护边界以及终端安全构成较为严重的威胁。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为 1624 个。

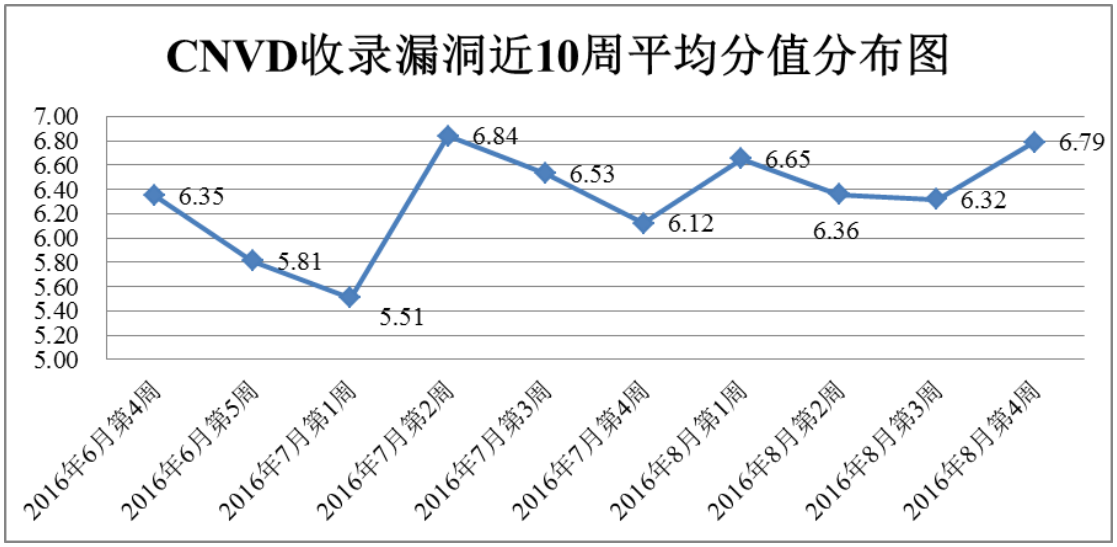

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 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 343 个漏洞。报送情况如表 1 所示。其中，安天实验室、绿盟科技、恒安嘉新、H3C 等单位报送数量较多。奇虎（补天平台）、漏洞盒子、深圳市深信服电子科技有限公司、腾讯玄武实验室、中国航天科工四院软件评测中心、卫士通信息产业股份有限公司、广

州神月信息安全技术有限公司、太极计划及其他个人白帽子向 CNVD 提交了 1624 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）	1490	1490
安天实验室	140	0
绿盟科技	128	0
恒安嘉新	116	2
H3C	88	0
启明星辰	84	0
东软	66	1
天融信	43	2
中国电信集团系统集成有限责任公司	38	0
杭州安恒信息技术有限公司	35	0
漏洞盒子	38	38
深圳市深信服电子科技有限公司	24	24
腾讯玄武实验室	5	5
广州神月信息安全技术有限公司	4	4
中国航天科工四院软件评测中心	3	3
卫士通信息产业股份有限公司	3	3
太极计划漏洞平台	1	1
CNCERT 安徽分中心	5	5
CNCERT 上海分中心	2	2
CNCERT 云南分中心	1	1
个人	43	43

报送总计	2357	1624
录入总计	343（去重）	1624

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 343 个漏洞。其中应用程序漏洞 164 个，web 应用漏洞 134 个，安全产品 18 个，网络设备漏洞 16 个，操作系统漏洞 11 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	164
web 应用漏洞	134
安全产品漏洞	18
网络设备漏洞	16
操作系统漏洞	11

表 2 漏洞按影响类型统计表

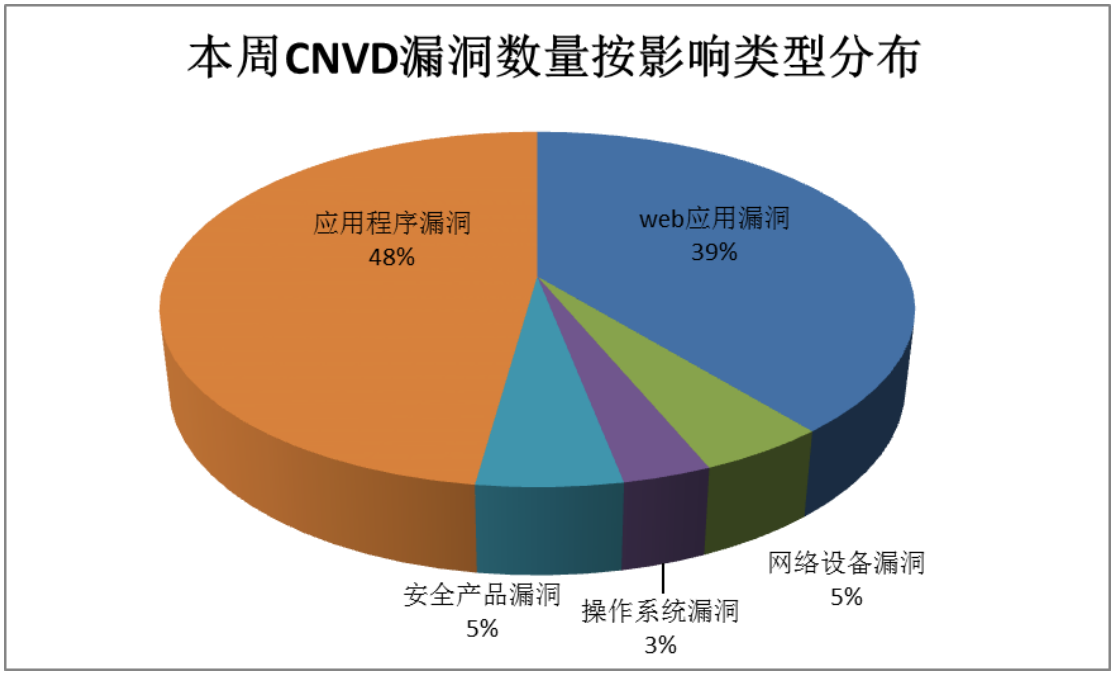

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 IBM、Huawei、Cybozu 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	15	4%
2	Huawei	11	3%

3	Cybozu	8	2%
4	Facebook	6	2%
5	Adobe	6	2%
6	SAP	4	1%
7	Drupal	4	1%
8	Apple	3	1%
9	WordPress	3	1%
10	其他	283	83%

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 16 个电信行业漏洞，7 个移动互联网行业漏洞（如下图所示）。其中，“Apple iOS kernel 存在内存破坏漏洞、Apple iOS WebKit 内存破坏漏洞、Legba Incorporated YateBTS 存在堆栈缓冲区溢出漏洞、Legba Incorporated YateBTS 存在设计漏洞、Legba Incorporated YateBTS 存在身份验证漏洞、OsmoCOM Osmo-TRX/Osmo-BTS 存在堆栈缓冲区溢出漏洞、OsmoCOM Osmo-TRX/Osmo-BTS 存在设计漏洞、OsmoCOM Osmo-TRX/Osmo-BTS 存在身份验证漏洞、Range Networks OpenBTS/OpenBTS-UMTS 存在设计漏洞、Range Networks OpenBTS/OpenBTS-UMTS 存在身份验证漏洞等”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/

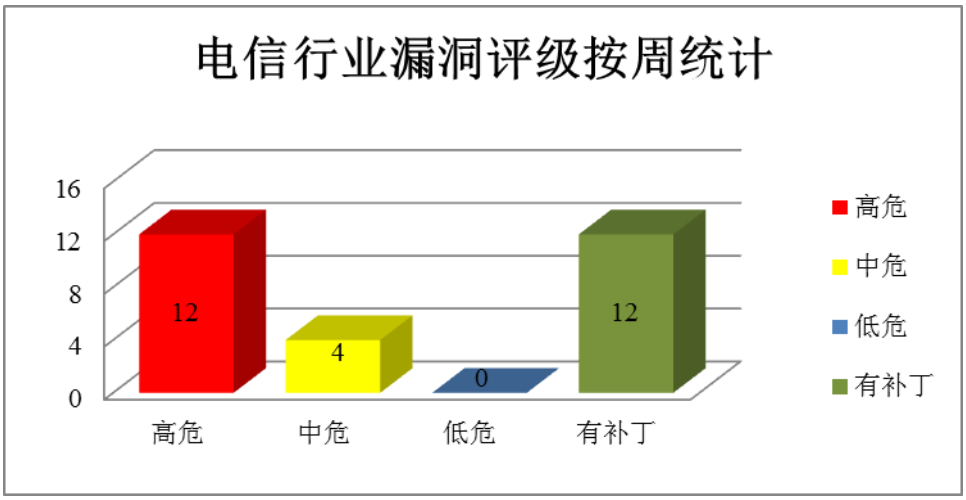

图 3 电信行业漏洞统计

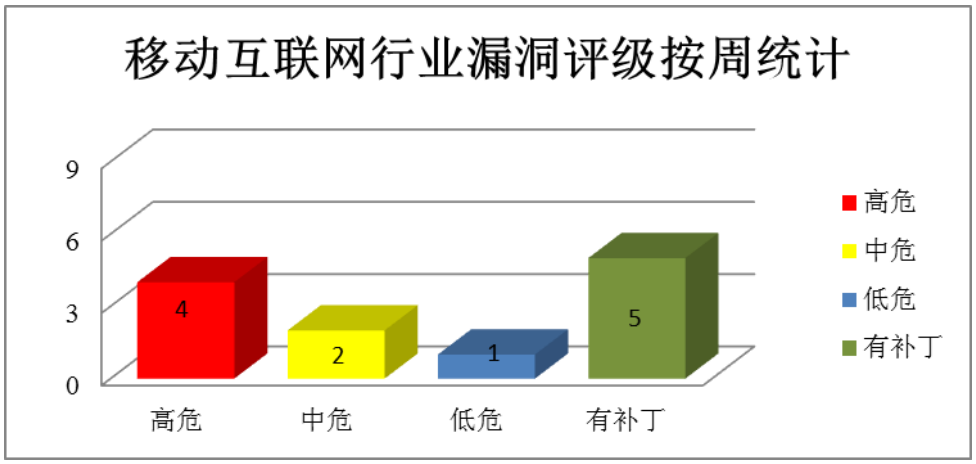

图 4 移动互联网行业漏洞统计

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、IBM 产品安全漏洞

IBM Connections 是美国 IBM 公司一套社交软件平台。本周，上述产品被披露存在跨站脚本漏洞，攻击者可利用漏洞注入任意 JavaScript 代码。

CNVD 收录的相关漏洞包括：IBM Connections 跨站脚本漏洞（CNVD-2016-06646、CNVD-2016-06647、CNVD-2016-06650、CNVD-2016-06697、CNVD-2016-06537、CNVD-2016-06536、CNVD-2016-06535、CNVD-2016-06533）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-2016-06646
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06647
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06650
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06697
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06537
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06536
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06535
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06533

2、Huawei 产品安全漏洞

Huawei UMA（Unified Maintenance and Audit ）是为运营商、政府、金融、电力、大企业等设计的统一 IT 核心资源运维管理与安全审计平台。Huawei Policy Center 是中国华为（Huawei）公司的一套策略管理中心软件。Huawei FusionCompute 是一套基于 Xen 开源设计的企业级开放式服务器虚拟化解决方案。Huawei FusionSphere 是华为自主知识产权的云操作系统。Huawei E9000 Chassis 是中国华为（Huawei）公司的一款刀片

服务器。Huawei AR 120 等都是 AR 系列企业路由器产品。Huawei Access Controllers AC6003 等都是无线接入控制器。OceanStor ISM 是一款集成系统管理软件 ，能够管理 CSS，可以查看 CSS 的告警和一些基本信息，并做一些基本的配置等。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、绕过安全限制或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Huawei UMA 信息泄露漏洞、Huawei Policy Center 跨站脚本漏洞、Huawei FusionCompute 信息泄露漏洞、Huawei FusionSphere 'Xenstore' 信息泄露漏洞、Huawei E9000 Chassis XML 外部实体注入漏洞、Huawei UMA 安全绕过漏洞、多款 Huawei 产品拒绝服务漏洞（CNVD-2016-06549）、Huawei OceanStor ISM 产品跨站脚本漏洞等。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-2016-06753
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06764
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06756
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06761
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06760
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06763
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06549
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06505

3、Cybozu 产品安全漏洞

Cybozu Garoon 是日本才望子（Cybozu）公司的一套门户型 OA 办公系统。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞绕过身份验证、执行任意脚本代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cybozu Garoon 访问权限绕过漏洞、Cybozu Garoon 身份验证绕过漏洞、Cybozu Garoon SQL 注入漏洞、Cybozu Garoon 开放重定向漏洞（CNVD-2016-06711）、Cybozu Garoon 跨站脚本漏洞（CNVD-2016-06712、CNVD-2016-06713、CNVD-2016-06714、CNVD-2016-06715）。其中，“Cybozu Garoon SQL 注入漏洞”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-2016-06708
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06709
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06710
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06711
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06712
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06713

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06714

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06715

4、Facebook 产品安全漏洞

Facebook HHVM（又名 HipHop Virtual Machine）是美国 Facebook 公司的一款能够显著提高 PHP 加载动态页面性能的虚拟机。本周，该产品被披露存在整数溢出漏洞和拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Facebook HHVM 存在多个漏洞（CNVD-2016-06542、CNVD-2016-06543、CNVD-2016-06544、CNVD-2016-06545、CNVD-2016-06546）、Facebook HHVM 存在多个漏洞。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-2016-06542

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06543

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06544

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06545

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06446

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06547

5、WatchGuard RapidStream 权限提升漏洞

WatchGuard RapidStream 是美国 WatchGuard 公司的一款防火墙设备。本周，WatchGuard RapidStream 被披露存在权限提升漏洞。攻击者可利用漏洞获取权限，执行任意命令。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-2016-06767

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-2016-06538	多款 F5 产品权限获取漏洞（CNVD-2016-06538）	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.f5.com/kb/en-us/solutions/public/k/12/sol12401251.html
CNVD-2016-06555	F5 BIG-IP Configuration Utility 存在未明漏洞	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.f5.com/kb/en-us/solutions/public/k/31/sol31925518.html
CNVD-2016-06564	Trend Micro Control Manager SQL 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，详情请关注厂商主页：http://www.trendmicro.com/

CNVD-2016-06565	Trend Micro Control Manager 存在多个 SQL 注入漏洞	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://esupport.trendmicro.com/solution/en-US/1114749.aspx
CNVD-2016-06570	多款 F5 产品存在未明漏洞	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.f5.com/kb/en-us/solutions/public/k/10/sol10133477.html
CNVD-2016-06569	OpenSSH 'crypt()'函数拒绝服务漏洞	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.openssh.com/txt/release-7.3
CNVD-2016-06641	Apache Ranger HTML 注入漏洞	高	目前厂商已经发布更新，详情请关注厂商主页或有关网址：https://cwiki.apache.org/confluence/display/RANGER/0.6.1+Release+-+Apache+Ra
CNVD-2016-06703	多款 Moxa 产品权限获取漏洞	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：http://www.moxa.com/product/moxa_device_manager.htm
CNVD-2016-06699	WordPress Zero Spam 插件 SQL 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://wpvulndb.com/vulnerabilities/8608
CNVD-2016-06768	ownCloud Desktop Client 本地命令注入漏洞	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://owncloud.org/security/advisory/?id=oc-sa-2016-016

表 4 部分重要高危漏洞列表

小结：本周，IBM 产品被披露存在跨站脚本漏洞，攻击者可利用漏洞注入任意 JavaScript 代码。此外，Huawei、Cybozu、Facebook 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞绕过安全限制、泄露敏感信息或发起拒绝服务攻击等。另外，有多款 F5 公司产品被披露存在高危漏洞。攻击者可利用漏洞获取权限，执行任意命令。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. 微信曝远程任意代码执行漏洞，可被远程控制

近日，360 手机卫士阿尔法团队（AlphaTeam）独家发现微信远程任意代码执行漏洞，将其命名为 badkernel。360 手机卫士阿尔法团队发现，通过此漏洞攻击者可获取微

信的完全控制权，危及用户朋友圈、好友信息、聊天记录甚至是微信钱包，可使上亿微信用户受到影响，危害巨大。目前，阿尔法团队的相关研究人员已经将此漏洞报告给腾讯应急响应中心并提供了修复建议。安全专家提醒用户，在耐心等待更新的同时请紧遵三个不要，不要随便扫描二维码，不要随意点击朋友圈链接，不要随意点击微信群内的链接，以防微信被远程控制。

参考链接：http://www.freebuf.com/news/112613.html

2. 【快讯】iOS 曝严重安全漏洞：iPhone 用户或已被监听数年

iOS 9.3.5 今天紧急上线，苹果更新日志中有提到修复了“重要安全问题”。如果你还没有更新的话，那么请尽快更新，因为这次涉及的 iOS 安全问题可能是“前所未有”的。苹果所指的重要安全问题乃是说 3 个 0-day 漏洞，这 3 个漏洞足以让攻击者对全球范围内的 iPhone 进行监听。利用这 3 个漏洞的是款软件套装，名为 Pegasus。Pegasus 影响的 iOS 版本，从最近的 iOS 9.3.4 一直到较早的 iOS 7，这表明 Pegasus 可能已经在人类毫不知情的情况下，持续监听了 iOS 用户好几年时间，直到最近才被发现。所以对 iPhone 和 iPad 用户而言，还是赶紧升级最新版的 iOS 9.3.5 吧，未知最新 iOS 10 预览版是否也存在这些漏洞。FreeBuf 后续还将针对此次事件进行更为详细的报道。

参考链接：http://www.freebuf.com/news/112967.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