

信息安全漏洞周报

2015 年 01 月 19 日-2015 年 01 月 25 日

2015 年第 4 期

本周漏洞基本情况

本周信息安全漏洞威胁整体评价级别为**低**。

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 166 个，其中高危漏洞 36 个、中危漏洞 114 个、低危漏洞 16 个。上述漏洞中，可利用来实施远程攻击的漏洞有 138 个。本周收录的漏洞中，已有 140 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。本周互联网上出现“Mac roplant iExplorer 不可信搜索路径漏洞”、“WordPress 插件 WP Symposium 存在多个任意文件上传漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 7 家成员单位及个人报送了本周收录的全部 166 个漏洞。报送情况如表 1 所示。其中，奇虎 360、天融信、安天实验室、启明星辰、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、上海天泰网络科技有限公司及白帽子向 CNVD 提交了多个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	1114	1114
天融信	231	0
安天实验室	200	0
启明星辰	183	0
恒安嘉新	111	0
绿盟科技	78	0

东软	1	0
上海天泰网络技术有限公司	1	1
CNCERT 江西分中心	5	5
CNCERT 福建分中心	3	3
CNCERT 河南分中心	3	3
个人	4	4
报送总计	1934	1130
录入总计	166（去重）	1130

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、Drupal、Cisco 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	Oracle	69	42%
2	Drupal	9	5%
3	Cisco	7	4%
4	Symantec	5	3%
5	Juniper Networks	5	3%
6	Django Software Foundation	4	2%
7	WordPress	3	2%
8	McAfee	3	2%
9	IBM	3	2%
10	其他	58	35%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 166 个漏洞。其中应用程序漏洞 100 个，WEB 应用漏洞 24 个，操作系统漏洞 22 个，数据库漏洞 8 个，安全产品漏洞 8 个，网络设备漏洞 4 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	100

WEB 应用漏洞	24
操作系统漏洞	22
数据库漏洞	8
安全产品漏洞	8
网络设备漏洞	4

表 3 漏洞按影响类型统计表

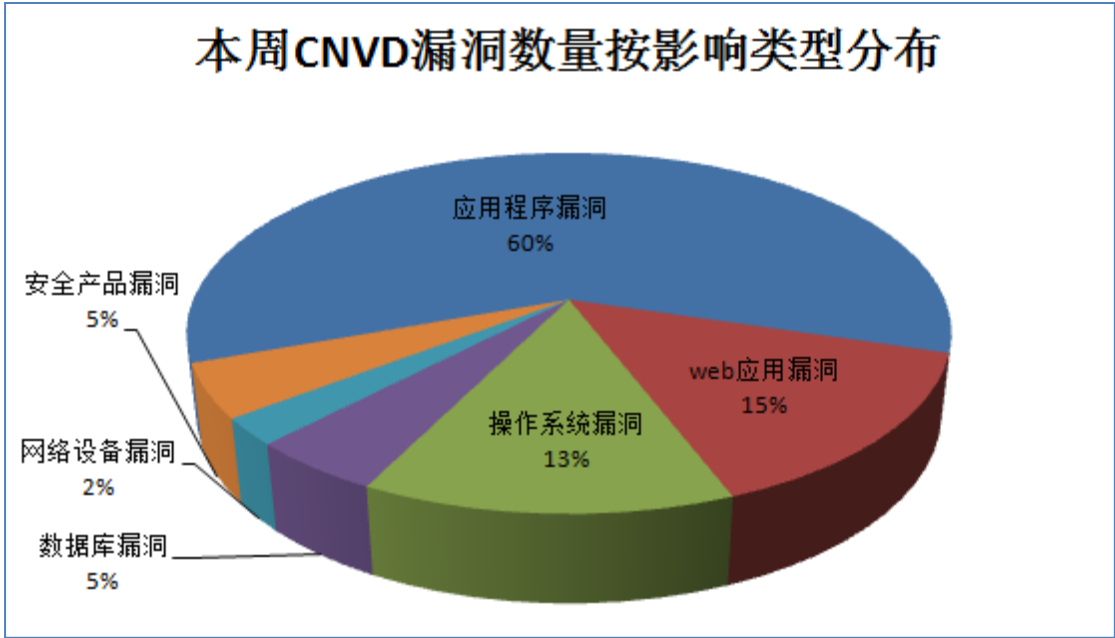


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 20 个电信行业漏洞，6 个工控系统行业漏洞（如下图表所示）。其中，“Juniper Junos JPPP Daemon 远程拒绝服务漏洞、Juniper Junos 远程拒绝服务漏洞（CNVD-2015-00383）、Arbiter Systems GPS Clock 存在漏洞、Oracle Database Server 远程漏洞（CNVD-2015-00487）、Clorius Controls A/S Java Web 客户端信息泄露漏洞、Schneider Electric ETG3000 FactoryCast HMI Gateway FTP 内置密码漏洞”的综合评级均为“高危”。相关厂商已经发布了上述漏洞的修补程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2015-00386	Juniper Junos 本地权限提升漏洞	中	是
电信	CNVD-2015-00385	Juniper Junos 拒绝服务漏洞（CNVD-2015-00385）	中	是
电信	CNVD-2015-00384	Juniper Junos 安全绕过漏洞（CNVD-2015-00384）	中	是
电信	CNVD-2015-00387	Juniper Junos JPPP Daemon 远程拒绝服务漏洞	高	是
电信	CNVD-2015-00383	Juniper Junos 远程拒绝服务漏洞（CNV	高	是

		D-2015-00383)		
电信	CNVD-2015-00409	ASUSWRT 后门命令执行漏洞	高	否
电信	CNVD-2015-00427	Cisco AnyConnect Secure Mobility Client 身份欺骗漏洞	中	否
电信	CNVD-2015-00450	多个 General Electric(GE)产品存在拒绝服务漏洞	中	是
电信	CNVD-2015-00442	Arbiter Systems GPS Clock 存在漏洞	高	是
电信	CNVD-2015-00468	Oracle Database Server 远程漏洞 (CNVD-2015-00468)	中	是
电信	CNVD-2015-00470	Oracle Database Server 远程漏洞 (CNVD-2015-00470)	中	是
电信	CNVD-2015-00487	Oracle Database Server 远程漏洞 (CNVD-2015-00487)	高	是
电信	CNVD-2015-00488	Oracle WebLogic Server 远程漏洞	中	是
电信	CNVD-2015-00490	Oracle Database Server 远程漏洞 (CNVD-2015-00490)	中	是
电信	CNVD-2015-00472	Oracle Database Server 远程漏洞 (CNVD-2015-00472)	中	是
电信	CNVD-2015-00473	Oracle Database Server 远程漏洞 (CNVD-2015-00473)	低	是
电信	CNVD-2015-00499	Oracle SOA Suite B2B Engine 子件存在未明漏洞	中	是
电信	CNVD-2015-00506	Oracle Reports Developer 存在未明漏洞	中	是
电信	CNVD-2015-00530	Oracle Database Server OJVM 组件存在未明漏洞	中	是
电信	CNVD-2015-00531	Oracle Database Server Workspace Manager 组件存在未明漏洞	中	是
工控系统	CNVD-2015-00404	Clorius Controls A/S Java Web 客户端信息泄露漏洞	高	是
工控系统	CNVD-2015-00424	Siemens SIMATIC WinCC Sm@rtClient app 信息泄露漏洞	中	是
工控系统	CNVD-2015-00425	Siemens SIMATIC WinCC Sm@rtClient app 本地安全绕过漏洞	中	是
工控系统	CNVD-2015-00426	Siemens SIMATIC WinCC Sm@rtClient app 信息泄露漏洞 (CNVD-2015-00426)	中	是
工控系统	CNVD-2015-00443	GE Proficy HMI/SCADA-CIMPLICITY 存在多个本地缓冲区溢出漏洞	中	是
工控系统	CNVD-2015-00498	Schneider Electric ETG3000 FactoryCast HMI Gateway FTP 内置密码漏洞	高	是

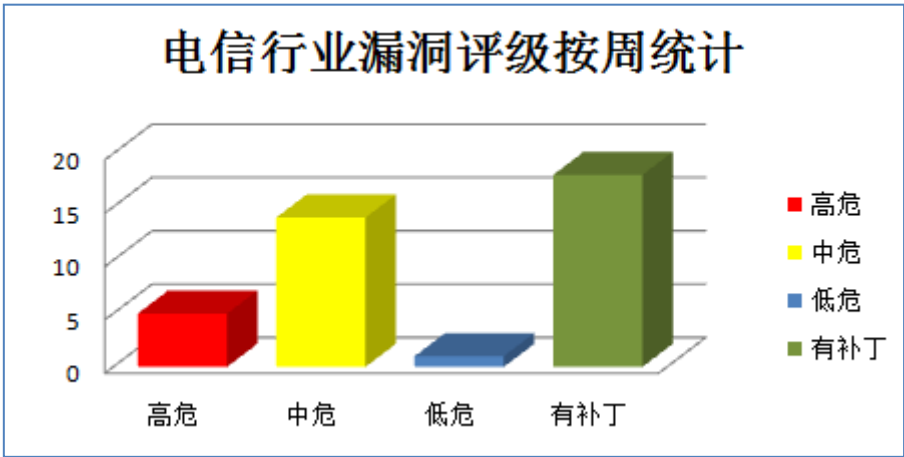


图 1 电信行业漏洞统计

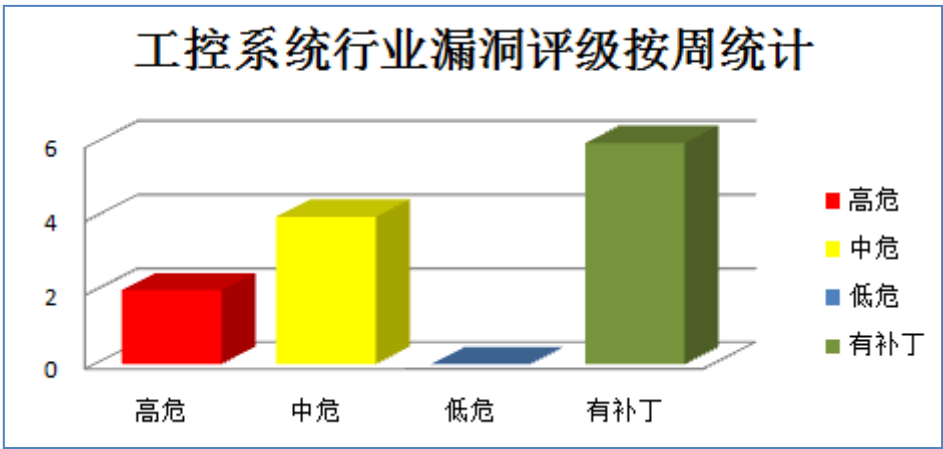


图 2 工控系统行业漏洞统计



本周重要漏洞信息

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、Oracle 产品安全漏洞

1 月 20 日，Oracle 发布了 2015 年 1 月份的安全更新，修复了其多款产品存在的 169 个安全漏洞。受影响的产品包括 Oracle 数据库（8 个）、中间件产品 Fusion Middleware（36 个）；Oracle Siebel 托管型 CRM 软件（17 个）、电子商务套装软件 Oracle E-Business Suite（10 个）、企业管理器网格控制产品 Oracle Enterprise Manager Grid Control（10 个）、供应链套装软件 Oracle Supply Chain Products Suite（6 个）；Virtualization（11 个）、PeopleSoft 产品（7 个）、JD Edwards 产品（1 个）、iLearning（2 个）、Communications Applications（2 个）、Retail Applications（1 个）、Health Sciences Applications（1 个）、JavaSE（19 个）、Oracle Sun 系统产品（29 个）和 MySQL 数据库（9 个）。本

次安全更新提供了针对 28 个高危漏洞的补丁，有 142 个漏洞可被远程利用。CNVD 提醒广大 Oracle 用户，请及时下载补丁更新，避免引发漏洞相关的安全事件。

CNVD 收录的相关漏洞包括：Oracle JD Edwards EnterpriseOne Tools 组件存在未明漏洞、Oracle Communications Applications 存在未明漏洞、Oracle Solaris 存在未明漏洞（CNVD-2015-00469、CNVD-2015-00465）、Oracle Java SE 存在远程漏洞（CNVD-2015-00477）、Oracle Solaris 存在未明漏洞（CNVD-2015-00489）、Oracle Database Server 远程漏洞（CNVD-2015-00487）、Oracle GlassFish Server 远程漏洞。上述漏洞的综合评级均为“高危”。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，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/3569>

2、Cisco 产品安全漏洞

Cisco Unified Communications 是一款 Cisco IP 电话解决方案中的呼叫处理组件。Cisco Identity Services Engine 身份服务引擎一款用于 Cisco TrustSec 解决方案的中央策略引擎。Cisco AsyncOS 是 Cisco 为全部邮件应用的性能和安全而专门定制的操作系统。Cisco Adaptive Security Appliance Software 是可提供安全和 VPN 服务的模块化平台。Cisco TelePresence Video Communication Server 是一款整合 h.323 和 SIP 的视频会议解决方案。本周，上述产品被披露存在跨站脚本、跨站请求伪造和拒绝服务漏洞，攻击者可利用漏洞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：Cisco Unified Communications Domain Manager 跨站请求伪造漏洞、Cisco Identity Services Engine 存在多个跨站脚本漏洞（CNVD-2015-00393）、Cisco Unified Communications Domain Manager 远程拒绝服务漏洞（CNVD-2015-00394）、Cisco AsyncOS 存在多个跨站脚本漏洞、Cisco Adaptive Security Appliance Software 拒绝服务漏洞（CNVD-2015-00430）、Cisco TelePresence Video Communication Server/Expressway 拒绝服务漏洞。目前，厂商已经发布了上述漏洞的修补程序。CNVD 提醒用户尽快下载补丁更新，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-2015-00392>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00393>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00394>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00429>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00430>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00411>

3、Drupal 产品安全漏洞

Drupal 是一套用 PHP 语言开发的免费、开源的内容管理系统。本周，上述产品被披露存在跨站脚本和跨站请求伪造漏洞，攻击者可利用漏洞执行未授权操作或进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：Drupal Wishlist 模块跨站请求伪造漏洞、Drupal Tadaa! 模块存在多个跨站请求伪造漏洞、Drupal Room Reservations 模块存在多个跨站脚本漏洞、Drupal Term Merge 模块跨站脚本漏洞、Drupal Wishlist 模块跨站脚本漏洞、Drupal Video 模块存在多个跨站脚本漏洞、Drupal Contact Form Fields 存在多个跨站请求伪造漏洞、Drupal Content Analysis 模块跨站脚本漏洞。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-2015-00459>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00458>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00457>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00456>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00455>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00454>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00453>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00412>

4、Juniper Networks 产品安全漏洞

Juniper Networks JUNOS 是一款 Juniper 网络公司的系列边界路由器等所运行的操作系统。本周，上述产品被披露存在拒绝服务、安全绕过、权限提升漏洞，攻击者可利用漏洞提升权限、执行未授权操作或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Juniper Junos 远程拒绝服务漏洞（CNVD-2015-00383）、Juniper Junos JPPP Daemon 远程拒绝服务漏洞、Juniper Junos 安全绕过漏洞（CNVD-2015-00384）、Juniper Junos 拒绝服务漏洞（CNVD-2015-00385）、Juniper Junos 本地权限提升漏洞。其中“Juniper Junos 远程拒绝服务漏洞（CNVD-2015-00383）、Juniper Junos JPPP Daemon 远程拒绝服务漏洞”的综合评级均为“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-2015-00383>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00387>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00384>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00385>

<http://www.cnvd.org.cn/flaw/show/CNVD-2015-00386>

5、VLC Media Player '.flv'文件内存破坏漏洞

VLC Media Player 是一款流行的多媒体播放程序。本周，VLC Media Player 被披露存在综合评级为“高危”的内存破坏漏洞。攻击者可以利用漏洞执行任意代码或发起拒绝服务攻击。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-2015-00418>

更多高危漏洞如表 3 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-2015-00410	Phoenix Contact ProConOs and MultiProg 验证绕过漏洞	高	暂无
CNVD-2015-00423	Hancom Office 缓冲区溢出漏洞	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://archives.neohapsis.com/archives/bugtraq/2013-12/0100.html
CNVD-2015-00428	AlienVault OSSIM and USM 存在多个命令执行漏洞	高	AlienVault OSSIM and USM 4.15 已经修复该漏洞，建议用户下载更新： https://www.alienvault.com
CNVD-2015-00463	多个 Symantec 产品远程代码执行漏洞	高	用户可联系供应商获得补丁信息： http://www.symantec.com/index.jsp
CNVD-2015-00462	多个 Symantec 产品 SQL 注入漏洞	高	用户可联系供应商获得补丁信息： http://www.symantec.com/index.jsp
CNVD-2015-00475	ManageEngine ServiceDesk 远程代码执行漏洞	高	用户可联系供应商获得补丁信息： https://raw.githubusercontent.com/pedrib/PoC/master/ManageEngine/me_sd_file_upload.txt
CNVD-2015-00536	FFmpeg 'libavcodec/utvideodec.c' 拒绝服务漏洞	高	用户可联系供应商获得补丁信息： https://www.ffmpeg.org/
CNVD-2015-00537	FFmpeg 'vmd_decode'函数拒绝服务漏洞	高	用户可联系供应商获得补丁信息： https://www.ffmpeg.org/
CNVD-2015-00538	IBM BladeCenter SAS Connectivity Module 和 SAS RAID Module 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-947.ibm.com/support/entry/portal/docdisplay?lnocid=MIGR-5096774
CNVD-2015-00510	VLC Media Player 存在多个漏洞	高	VLC media player 2.1.5 已经修复该漏洞，建议用户下载更新： http://www.videolan.org/

表 3 部分高危漏洞列表

小结：1 月 20 日，Oracle 发布了 2015 年 1 月份的安全更新，修复了其多款产品存在的 169 个安全漏洞。本次安全更新提供了针对 28 个高危漏洞的补丁，有 142 个漏洞可被远程利用。此外，Cisco、Drupal、Juniper Networks 多款产品被披露存在多个安全漏洞，允许攻击者利用漏洞提升权限、执行未授权操作、进行跨站脚本攻击或发起拒绝服务攻击。另外，VLC Media Player 被披露存在一个高危零日漏洞。攻击者可以利用

漏洞执行任意代码或发起拒绝服务攻击。建议相关用户应随时关注上述厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、Linux 修补 Kernel 产品漏洞

Linux Kernel 是 Linux 操作系统的内核。

本周，Linux 修补了上述产品存在的安全绕过和信息泄露漏洞，避免攻击者利用漏洞绕过安全限制执行未授权操作和获取敏感信息。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/54122>
<http://www.cnvd.org.cn/patchInfo/show/54182>

本周要闻速递

1. 全球最大域名提供商 GoDaddy 存在跨站请求伪造（CSRF）漏洞

全球最大域名提供商 GoDaddy 存在跨站请求伪造（CSRF）漏洞，攻击者可利用该漏洞编辑域名服务，更改自动更新设置或者编辑域名内容。跨站请求伪造类似于跨站脚本漏洞（XSS），大多数时候，这类漏洞需要结合一些欺骗或者社会工程学方法才能造成危害。但这个漏洞由于牵扯到域名管理，所以相对来说比较严重。攻击者可以利用跨站请求伪造（CSRF）漏洞在用户不知情的情况下控制域名。

参考链接：<http://www.freebuf.com/news/57011.html>

2. 谷歌（Google）公布数个苹果 0day 漏洞

谷歌 Project Zero 漏洞研究团队公布了苹果数个 0day 漏洞及技术细节，该漏洞通过提升系统权限进而控制整个受害者 Mac 计算机。此外，就在两周前，谷歌刚刚披露了微软 Windows8.1 0day 漏洞，引发争议。谷歌在公开披露的漏洞报告里包含一个 POC（概念验证利用）代码，里面提供了足够多的技术细节，以至于攻击者可以重写代码发动有针对性的攻击。

参考链接：<http://www.freebuf.com/news/57304.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