

信息安全漏洞周报

2014 年 5 月 19 日-2014 年 5 月 25 日

2014 年第 21 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**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 66 个、中危漏洞 106 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 147 个。本周收录的漏洞中，已有 139 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“PH P-Nuke 'modules.php' SQL 注入漏洞”、“Clipperz Password Manager 'backend/php/src/setup/rpc.php' 远程代码执行漏洞”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 6 家成员单位、合作伙伴及个人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、启明星辰、天融信、绿盟等单位报送数量较多。此外，CNCERT 各分中心、习科网络安全及多个白帽子向 CNVD 提交了 98 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
安天实验室	194	0
启明星辰	111	0
天融信	103	0
绿盟科技	76	0
恒安嘉新	38	0
东软	3	0
习科网络安全	55	55
CNCERT 广东分中心	19	19

CNCERT 山东分中心	9	9
CNCERT 江西分中心	5	5
CNCERT 山西分中心	1	1
CNCERT 内蒙古分中心	1	1
CNCERT 宁夏分中心	1	1
CNCERT 天津分中心	1	1
CNCERT 福建分中心	1	1
CNCERT 安徽分中心	1	1
CNCERT 上海分中心	1	1
个人	3	3
报送总计	623	98
录入总计	183（去重）	98

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 QEMU、Cisco、IBM 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	QEMU	21	11%
2	Cisco	16	9%
3	IBM	13	7%
4	Google	9	5%
5	D-Link	7	4%
6	Moodle	6	3%
7	Mahara	4	2%
8	Solar-Log	3	2%
9	Microsoft	2	1%
10	其他	102	56%

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 183 个漏洞。其中应用程序漏洞 137 个，WEB 应用漏洞 23 个，网络设备漏洞 18 个，安全产品漏洞 3 个，操作系统漏洞 2 个。

漏洞影响对象类型	漏洞数量
----------	------

应用程序漏洞	137
WEB 应用漏洞	23
网络设备漏洞	18
安全产品漏洞	3
操作系统漏洞	2

表 3 漏洞按影响类型统计表

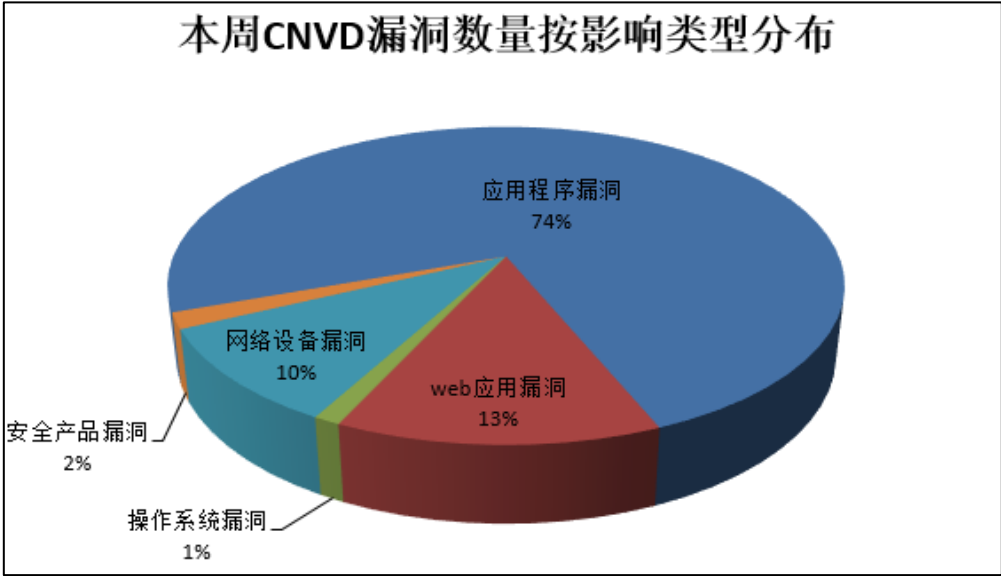


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 27 个电信行业漏洞、1 个移动互联网行业漏洞、2 个工控行业漏洞（如下列表所示）。其中，“IBM WebSphere Commerce 'id'参数处理拒绝服务漏洞、IBM WebSphere Application Server 拒绝服务漏洞（CNVD-2014-03209）、IBM Eclipse Help System 目录遍历漏洞、Cogent Real-Time Systems DataHub 'GetPermissions.asp' 远程代码执行漏洞、CSWorks LiveData Service Web API SQL 注入漏洞”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。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2014-03083	Cisco IOS/OS XE Software LISP 拒绝服务漏洞	中	是
电信	CNVD-2014-03081	D-Link DGL-5500 存在多个漏洞	中	是
电信	CNVD-2014-03069	D-Link DIR-855L 和 DIR-835 存在多个漏洞	中	是
电信	CNVD-2014-03084	IBM WebSphere Commerce 'id'参数处理拒绝服务漏洞	高	是

电信	CNVD-2014-03095	Cisco IOS XR Software SNMP 请求处理拒绝服务漏洞	中	是
电信	CNVD-2014-03118	IBM WebSphere Portal 存在未明拒绝服务漏洞	中	是
电信	CNVD-2014-03117	IBM WebSphere Portal filterform.jsp 存在未明跨站脚本漏洞	中	是
电信	CNVD-2014-03116	IBM WebSphere Portal boot_config.jsp 跨站脚本漏洞	中	是
电信	CNVD-2014-03115	IBM WebSphere Portal 存在多个漏洞	中	是
电信	CNVD-2014-03114	IBM WebSphere Portal Social Rendering 跨站脚本漏洞	低	是
电信	CNVD-2014-03113	IBM WebSphere Portal .jsp 跨站脚本漏洞	中	是
电信	CNVD-2014-03112	IBM WebSphere Portal 开放重定向漏洞	中	是
电信	CNVD-2014-03111	IBM WebSphere Portal 存在未明拒绝服务漏洞（CNVD-2014-03111）	中	是
电信	CNVD-2014-03142	TP-Link TD-W89 Routers 'rom-0'文件未授权访问漏洞	中	否
电信	CNVD-2014-03160	Cisco NX-OS Software 目录遍历漏洞	中	否
电信	CNVD-2014-03155	D-Link DWC-1000 'thispage' 目录遍历漏洞	中	是
电信	CNVD-2014-03189	Cisco IOS Software LLDP 请求处理拒绝服务漏洞	中	是
电信	CNVD-2014-03185	Cisco IOS RTCP Input Queue 拒绝服务漏洞	中	是
电信	CNVD-2014-03190	Cisco IOS XR Software DHCPv6 报文请求处理拒绝服务漏洞（CNVD-2014-03190）	中	是
电信	CNVD-2014-03191	Cisco IOS XR Software DHCPv6 报文请求处理拒绝服务漏洞（CNVD-2014-03191）	中	是
电信	CNVD-2014-03192	Cisco Security Manager 自动升级服务器跨站脚本漏洞	中	是
电信	CNVD-2014-03211	D-Link DAP-1150 跨站脚本漏洞	中	否
电信	CNVD-2014-03210	D-Link DAP-1150 跨站请求伪造漏洞（CNVD-2014-03210）	中	否
电信	CNVD-2014-03209	IBM WebSphere Application Server 拒绝服务漏洞（CNVD-	高	是

		2014-03209))		
电信	CNVD-2014-03208	IBM Eclipse Help System 目录遍历漏洞	高	是
电信	CNVD-2014-03207	IBM Eclipse Help System 跨站脚本漏洞	中	是
电信	CNVD-2014-03221	D-Link DIR-605L 路由器存在多个漏洞	中	否
移动互联网	CNVD-2014-03161	Bilyoner Applications SSL/TLS 验证绕过漏洞	中	是
工控系统	CNVD-2014-03106	Cogent Real-Time Systems DataHub 'GetPermissions.asp'远程代码执行漏洞	高	是
工控系统	CNVD-2014-03157	CSWorks LiveData Service Web API SQL 注入漏洞	高	是

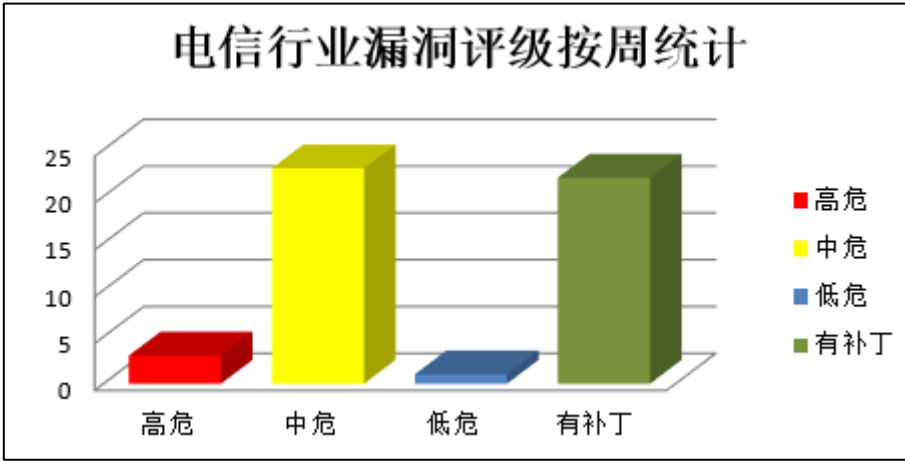


图 1 电信行业漏洞统计

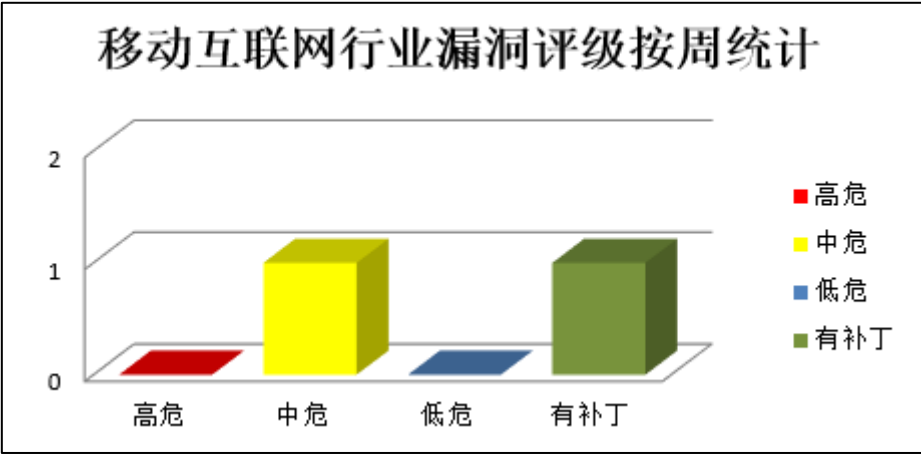


图 2 移动互联网行业漏洞统计

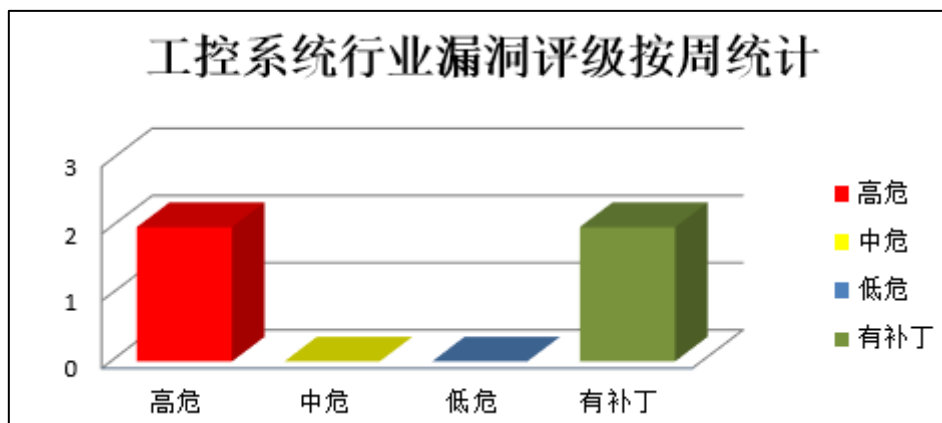


图 3 工控行业漏洞统计

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、Google 产品安全漏洞

Google Chrome 是一款流行的 WEB 浏览器。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞在浏览器上下文中执行任意代码，绕过安全限制，执行欺骗攻击或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Chrome V8 整数下溢漏洞、Google Chrome 存在多个内存破坏漏洞、Google Chrome SVG 处理内存错误引用漏洞、Google Chrome 音频处理整数溢出漏洞、Google Chrome 样式处理内存错误引用漏洞。上述漏洞的综合评级均为“高危”。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-2014-03230>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03231>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03237>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03234>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03233>

2、QEMU 产品安全漏洞

QEMU 是一款开源模拟器软件。本周，上述产品被披露存在内存破坏漏洞，攻击者可利用漏洞在受影响应用上下文中执行任意代码。

CNVD 收录的相关漏洞包括：QEMU 内存破坏漏洞（CNVD-2014-03120、CNVD-2014-03121、CNVD-2014-03122、CNVD-2014-03123、CNVD-2014-03124）。上述漏洞的综合评级均为“高危”。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-2014-03120>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03121>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03122>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03123>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03124>

3、IBM 产品安全漏洞

IBM Eclipse Help System (IEHS) 是美国 IBM 公司的一套用来制作 Eclipse 帮助系统的软件。IBM WebSphere Portal 提供了一个组合应用程序或业务框架，并且提供了一种高级工具来构造灵活的，基于 SOA 的解决方案。IBM WebSphere Commerce 是一款商务应用开发软件。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞通过精心编制的 URL 注入任意 WEB/HTML 脚本、读取任意文件或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM Eclipse Help System 目录遍历漏洞、IBM WebSphere Application Server 拒绝服务漏洞 (CNVD-2014-03209)、IBM WebSphere Commerce 'id' 参数处理拒绝服务漏洞、IBM Eclipse Help System 跨站脚本漏洞、IBM WebSphere Portal .jsp 跨站脚本漏洞。其中，除“IBM Eclipse Help System 跨站脚本漏洞、IBM WebSphere Portal .jsp 跨站脚本漏洞”外，其余漏洞的综合评级均为“高危”。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-2014-03208>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03209>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03084>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03207>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03113>

4、Cisco 产品安全漏洞

Cisco IOS 是多数思科系统路由器和网络交换机上使用的互联网络操作系统。本周，上述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。

CNVD 收录的相关漏洞包括：Cisco IOS RTCP Input Queue 拒绝服务漏洞、Cisco IOS XR Software DHCPv6 报文请求处理拒绝服务漏洞 (CNVD-2014-03191、CNVD-2014-03190)、Cisco IOS Software LLDP 请求处理拒绝服务漏洞、Cisco IOS XR Software SNMP 请求处理拒绝服务漏洞。厂商已发布了上述漏洞的修补程序。CNVD 提醒相关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-2014-03185>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03191>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03190>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03189>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-03095>

5、RealPlayer '.3gp'文件处理内存破坏漏洞

RealNetworks RealPlayer 是一款流行的媒体播放程序。本周，RealPlayer 被披露存在综合评级为“高危”的内存破坏漏洞。允许攻击者利用漏洞构建恶意文件，诱使用户解析，可使应用程序崩溃或执行任意代码。目前，互联网上已经出现了针对该漏洞的攻击代码，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-2014-03147>

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-2014-03082	CodeIgniter/Kohana 'unserialize()' 函数 PHP 对象注入漏洞	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： https://github.com/kohana/core/pull/492
CNVD-2014-03070	Codem-transcode 'lib/probe-handler.js'远程命令注入漏洞	高	Codem-transcode 0.5.0 已经修复该漏洞，建议用户下载更新： http://www.transcodem.com
CNVD-2014-03071	Etherpad Lite ep_imageconvert 插件远程命令注入漏洞	高	Etherpad Lite ep_imageconvert 0.0.3 已经修复该漏洞，建议用户下载更新： https://github.com/ether/etherpad-lite
CNVD-2014-03072	FreeBSD pkg Bootstrap 工具签名校验漏洞	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://www.freebsd.org/security/advisories/FreeBSD-EN-14%3a03.pkg.asc
CNVD-2014-03074	Hubot Scripts 'email.coffee'模块远程命令注入漏洞	高	Hubot Scripts > 2.4.4 已经修复该漏洞，建议用户下载更新： https://github.com/github/hubot-scripts/
CNVD-2014-03076	Marked 模块远程命令注入漏洞	高	Marked Module 0.3.1 已经修复该漏洞，建议用户下载更新： https://www.npmjs.org/package/marked
CNVD-2014-03068	node-libnotify 'libnotify.notify'远程命令注入漏洞	高	node-libnotify 1.0.4 已经修复该漏洞，建议用户下载更新： https://github.com/mytrile/node-libnotify

CNVD-2014-03067	node-printer 'printDirect()'函数远程命令注入漏洞	高	node-printer > 0.0.1 已经修复该漏洞，建议用户下载更新： https://github.com/tojocky/node-printer
CNVD-2014-03058	ZamFoo 'accounttorestore'和'accounttochange'命令注入漏洞	高	暂无
CNVD-2014-03087	Solar-Log 未验证文件上传任意代码执行漏洞	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://www.solar-log.com/en/home.html

表 3 部分高危漏洞列表

小结：本周，Google 披露多个安全产品漏洞，攻击者可利用漏洞在浏览器上下文中执行任意代码，绕过安全限制，执行欺骗攻击或发起拒绝服务攻击。此外，QEMU、IBM、Cisco 集中披露多款产品存在多个漏洞，攻击者可利用漏洞执行任意代码或发起拒绝服务攻击。RealPlayer 被披露存在一个高危零日漏洞，攻击者可利用漏洞构建恶意文件，诱使用户解析，可使应用程序崩溃或执行任意代码。CNVD 已经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、Microsoft 修补 Debug Interface Access SDK 产品漏洞

Microsoft Debug Interface Access SDK 是一个调试接口组件。

本周，Microsoft 修补了上述产品存在的内存破坏漏洞，避免远程攻击者利用漏洞使应用程序崩溃或可执行任意代码。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/45680>

本周要闻速递

1. Linux 内核严重安全漏洞被发现

据报道，一个自 2009 年以来隐藏 5 年之久的 Linux 内核严重安全漏洞被发现，虽然目前该问题已经修复，却着实让 Linux 用户感到害怕，这样一个严重的漏洞居然五年才发现，这种情况在 Windows 系统下是不敢想象的。此 bug 是一个本地权限提升漏洞，管理员和用户都需要尽可能快的将系统更新到包含修正的最新版本。该 bug 是在 2

009 年发布的 2.6.31-rc3 中被引入到内核的，它存在于控制 Linux 伪 tty 设备的 `n_tty_write` 函数中，允许无特权的用户执行恶意代码。

参考链接: <http://server.zol.com.cn/454/4545485.html>

2. 苹果未修复 Windows iTunes SSL 漏洞

此前在 SSL 安全漏洞被披露之后，苹果很快就更新了 Mavericks 和 iOS，以保护用户免受该漏洞的影响。但是根据外媒的最新报道，如今即将过去两个月了，苹果还是没有修复 Windows iTunes 的漏洞，也就是说 Windows 用户如果使用 iTunes 会很容易因为 SSL 安全漏洞遭到攻击。根据此前的报道，黑客可以借助这一漏洞绕过 SSL/TLS 认证流程，导致 OS X 和 Windows 用户遭受“中间人”攻击。如果用户使用共享的有线或无线网络，就有可能导致通讯信息被黑客拦截，从而泄露敏感数据。

参考链接: <http://it.21cn.com/itnews/a/2014/0522/11/27289160.shtml>

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