国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 11 月 07 日-2016 年 11 月 13 日 **2016 年第 46 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 287 个，其中高危漏洞 146 个、中危漏洞 132 个、低危漏洞 9 个。漏洞平均分值为 6.82。本周收录的漏洞中，涉及 0day 漏洞 129 个（占 45%）。其中互联网上出现“Apple iOS 远程内存破坏漏洞、NodCMS PHP 代码执行漏洞”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 835 个，与上周（1000 个）环比增长 17%。

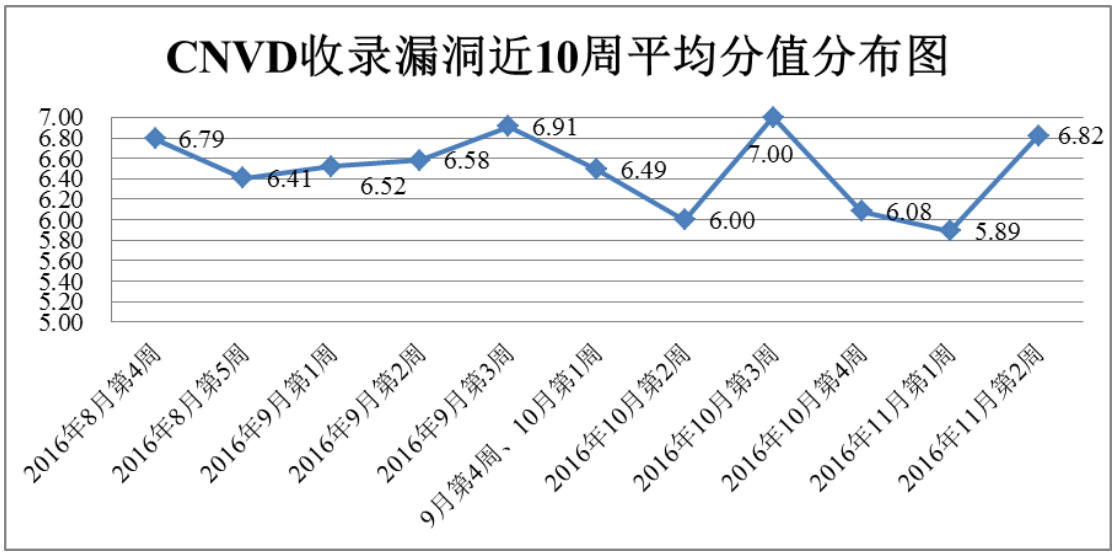

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 287 个漏洞。报送情况如表 1 所示。其中，恒安嘉新、安天实验室、绿盟科技、H3C、蓝盾信息安全技术有限公司等单位报送数量较多。360 网神、漏洞盒子、新疆天山智汇信

息科技有限公司、广西鑫瀚科技有限公司、南京铱迅信息技术股份有限公司、上海零盾网络科技有限公司、广州神月信息安全技术有限公司、中国航天科工集团第四研究院软件评测中心（北京）及其他个人白帽子向 CNVD 提交了 835 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	641	641
恒安嘉新	245	10
安天实验室	113	0
绿盟科技	110	0
H3C	68	0
蓝盾信息安全技术有限公司	62	0
华为技术有限公司	50	0
杭州安恒信息技术有限公司	50	0
中国电信集团系统集成有限责任公司	22	0
卫士通信息产业股份有限公司	4	0
知道创宇	3	0
启明星辰	1	1
漏洞盒子	124	124
新疆天山智汇信息科技有限公司	6	6
广西鑫瀚科技有限公司	5	5
南京铱迅信息技术股份有限公司	4	4
上海零盾网络科技有限公司	3	3
广州神月信息安全技术有限公司	2	2
中国航天科工集团第四研究院软件评测中	1	1

心（北京）		
CNCERT 宁夏分中心	4	4
个人	34	34
报送总计	1552	835
录入总计	287（去重）	835

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 287 个漏洞。其中 web 应用漏洞 127 个，应用程序漏洞 122 个，操作系统漏洞 18 个，网络设备漏洞 11 个，数据库漏洞 8 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
web 应用漏洞	127
应用程序漏洞	122
操作系统漏洞	18
网络设备漏洞	11
数据库漏洞	8
安全产品漏洞	1

表 2 漏洞按影响类型统计表

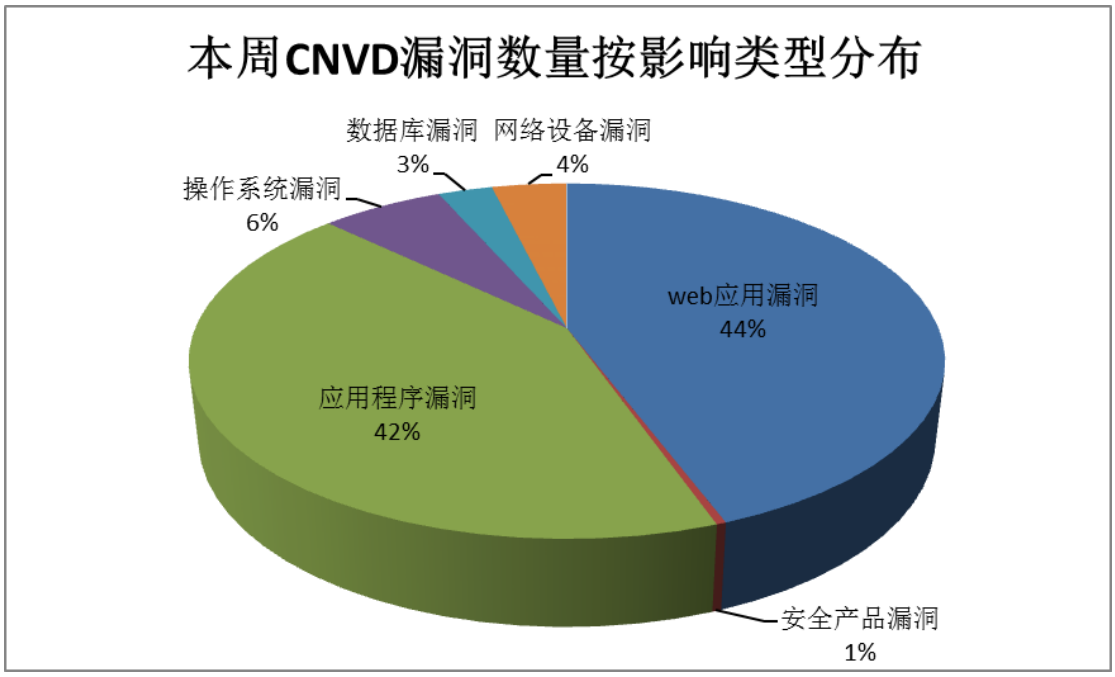

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Microsoft、Wordpress、OIC 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	Microsoft	48	17%
2	Wordpress	24	8%
3	OIC	16	6%
4	cURL	8	3%
5	IBM	6	2%
6	phpMyAdmin	6	2%
7	NVIDIA	4	1%
8	Google	3	1%
9	Cisco	3	1%
10	其他	169	59%

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 3 个电信行业漏洞，4 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图所示）。其中，“Apple iOS/macOS 本地代码执行漏洞、Samsung Mobile 拒绝服务漏洞”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/

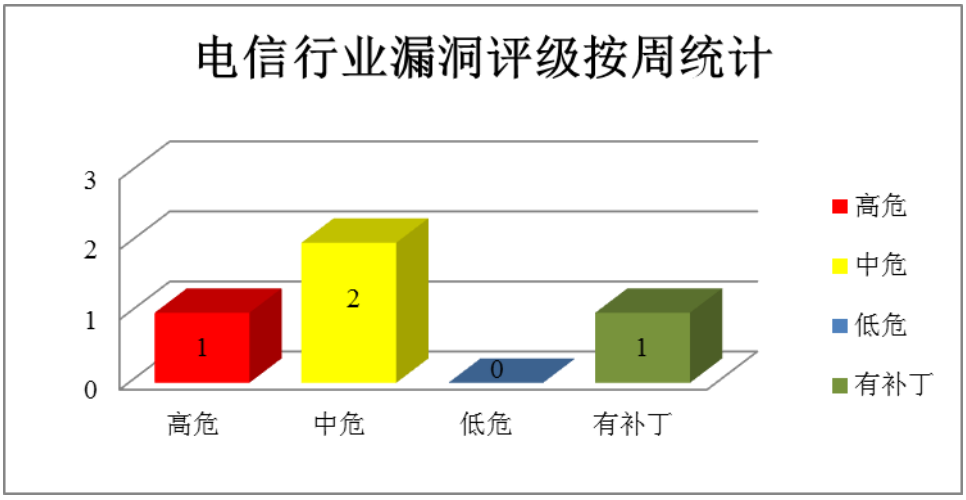

图 3 电信行业漏洞统计

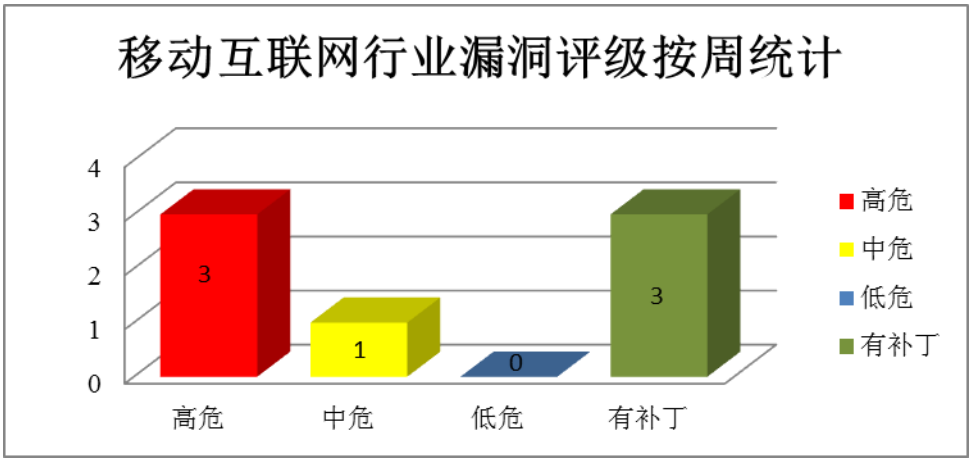

图 4 移动互联网行业漏洞统计

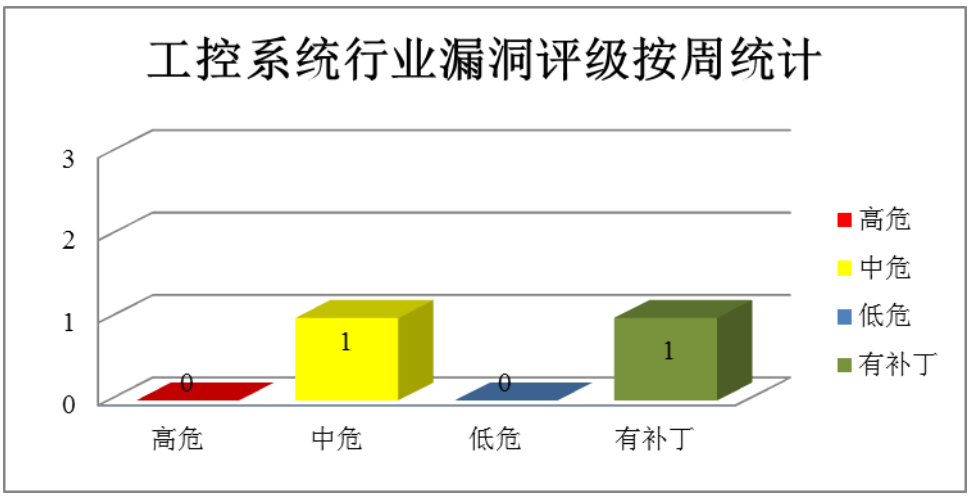

图 5 工控系统行业漏洞统计

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

11 月 8 日，微软发布了 2016 年 11 月份的月度例行安全公告，共含 14 项更新，修复了 MicrosoftWindows、Internet Explorer、Edge、Office、Office Services、SQL Server 和 WebApps 中存在的 67 个安全漏洞。其中，5 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 提醒广大 Microsoft 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。

CNVD 收录的相关漏洞包括：Microsoft Office 内存破坏漏洞（CNVD-2016-10969、CNVD-2016-10968、CNVD-2016-10967、CNVD-2016-10966、CNVD-2016-10976、CNVD-2016-10975、CNVD-2016-10974、CNVD-2016-10973）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/webinfo/show/3970

2、Adobe 产品安全漏洞

Adobe Flash Player 是美国奥多比（Adobe）公司的一款跨平台、基于浏览器的多媒体播放器产品。本周，该产品被披露存在内存错误引用和远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Flash Player 内存错误引用漏洞（CNVD-2016-10916、CNVD-2016-10915、CNVD-2016-10914、CNVD-2016-10913、CNVD-2016-10912、CNVD-2016-10911）、Adobe Flash Player 类型混淆远程代码执行漏洞（CNVD-2016-10908、CNVD-2016-10909）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-2016-10916
http://www.cnvd.org.cn/flaw/show/CNVD-2016-10915
http://www.cnvd.org.cn/flaw/show/CNVD-2016-10914
http://www.cnvd.org.cn/flaw/show/CNVD-2016-10913
http://www.cnvd.org.cn/flaw/show/CNVD-2016-10912
http://www.cnvd.org.cn/flaw/show/CNVD-2016-10911
http://www.cnvd.org.cn/flaw/show/CNVD-2016-10908
http://www.cnvd.org.cn/flaw/show/CNVD-2016-10909

3、OIC 产品安全漏洞

Exponent CMS 是美国 OIC 集团公司的一套基于 PHP 的免费、开源的模块化内容管理系统（CMS）。本周，该产品被披露存在 SQL 注入漏洞，攻击者可利用漏洞控制应用程序，访问或修改数据。

CNVD 收录的相关漏洞包括：Exponent CMS 'version'参数 SQL 注入漏洞、Exponent CMS 'author'参数 SQL 注入漏洞、Exponent CMS 'src'参数 SQL 注入漏洞、Exponent CMS 'title'参数 SQL 注入漏洞、Exponent CMS 'username'参数 SQL 注入漏洞、Exponent CMS 'is_what'参数 SQL 注入漏洞、Exponent CMS 'version'参数 SQL 注入漏洞、Exponent CMS 'fileid'参数 SQL 注入漏洞等。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-2016-10672
http://www.cnvd.org.cn/flaw/show/CNVD-2016-10671
http://www.cnvd.org.cn/flaw/show/CNVD-2016-10670
http://www.cnvd.org.cn/flaw/show/CNVD-2016-10669
http://www.cnvd.org.cn/flaw/show/CNVD-2016-10678

http://www.cnvd.org.cn/flaw/show/CNVD-2016-10704

http://www.cnvd.org.cn/flaw/show/CNVD-2016-10703

http://www.cnvd.org.cn/flaw/show/CNVD-2016-10702

4、IBM 产品安全漏洞

IBM InfoSphere Information Server Framework（ISF）和 IBM InfoSphere Information Server on Cloud 是美国 IBM 公司的产品。IBM AIX 是一套 UNIX 操作系统。 IBM Campaign 是一套用于帮助营销人员设计、执行、衡量和优化营销广告的管理解决方案。IBM Rational Team Concert（RTC）是一套基于 Jazz 平台且支持分散团队进行实时相关协作的软件生命周期管理解决方案。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞提升权限或发起跨站脚本攻击等。

CNVD 收录的相关漏洞包括：IBM AIX lquerylv 本地提权漏洞、IBM Campaign 跨站脚本漏洞、IBM Rational Team Concert 跨站脚本漏洞（CNVD-2016-10752、CNVD-2016-10750）、IBM Rational Team Concert 注入漏洞、IBM InfoSphere Information Server Framework 和 IBM InfoSphere Information Server on Cloud 点击劫持漏洞。其中“IBM AIX lquerylv 本地提权漏洞、IBM Rational Team Concert 注入漏洞”的危害等级为“高级”。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-2016-10799

http://www.cnvd.org.cn/flaw/show/CNVD-2016-10753

http://www.cnvd.org.cn/flaw/show/CNVD-2016-10752

http://www.cnvd.org.cn/flaw/show/CNVD-2016-10751

http://www.cnvd.org.cn/flaw/show/CNVD-2016-10750

http://www.cnvd.org.cn/flaw/show/CNVD-2016-10749

5、NodCMS PHP 代码执行漏洞

NodCMS 是一套免费的支持多语种的 PHP 开发框架。本周，NodCMS 被披露存在代码执行漏洞。攻击者可利用该漏洞在受影响应用程序上下文中执行任意代码，也可能造成拒绝服务。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-2016-10802

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-2016-10698	SAP Adaptive Server Enterprise 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://go.sap.com/
CNVD-2016-10730	Moxa OnCell Series 产品 OS 命令执行漏洞	高	目前厂商已经发布更新修复该漏洞，详情请关注厂商主页：http://www.moxa.com/
CNVD-2016-10738	git-fastclone 任意命令执行漏洞	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://github.com/square/git-fastclone/pull/2
CNVD-2016-10737	git-fastclone 命令执行漏洞	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://github.com/square/git-fastclone/pull/5
CNVD-2016-10735	Ansible 远程命令注入漏洞	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://bugzilla.redhat.com/show_bug.cgi?id=1388113
CNVD-2016-10748	Oracle MySQL、MariaDB 和 PerconaDB 提权漏洞	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.mysql.com/https://mariadb.org/https://www.percona.com/
CNVD-2016-10754	Sophos Web Appliance 4.2.1.3 版本权限提升漏洞	高	用户可升级至 4.3 版本，参考如下下载地址：http://swa.sophos.com/rn/swa/concepts/ReleaseNotes_4.3.html
CNVD-2016-10755	Sophos Web Appliance 4.2.1.3 版本远程代码执行漏洞	高	用户可升级至 4.3 版本，参考如下下载地址：http://swa.sophos.com/rn/swa/concepts/ReleaseNotes_4.3.html
CNVD-2016-10772	Zabbix 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，详情请关注厂商主页：http://www.zabbix.org/wiki/Main_Page
CNVD-2016-10957	Piwik PHP 对象注入漏洞	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://piwik.org/

表 4 部分重要高危漏洞列表

小结：11 月 8 日，微软发布了 2016 年 11 月份的月度例行安全公告，共含 14 项更新，修复了 MicrosoftWindows、Internet Explorer、Edge、Office、Office Services、SQL Server 和 WebApps 中存在多个漏洞。攻击者可提升权限，远程执行任意代码。此外，Adobe、OIC、IBM 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞执行任意代码、提升权限或发起跨站脚本攻击等。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. Gmail 存高危漏洞，用户帐号可被轻松破解

日前，来自巴基斯坦的一名学生以及安全研究人员在 Gmail 上发现了一个高危漏洞，它可以让黑客轻松劫持任何 Gmail 邮箱帐号。攻击者企图通过向 Google 发送邮件获取某一邮箱账号的所有权。Google 会向该邮件地址发送一封认证邮件进行验证。但由于该邮箱账号无法收取该封邮件，于是 google 的邮件就会发回到实际发送者（即黑客）手中，（此时）邮件中则还提供了验证码。黑客就可以利用这个验证码并获得该账号的所有权。

参考链接：http://www.freebuf.com/news/119229.html

2. 数十亿 Android App 账户存泄露风险

香港大学的三名安全研究人员发现，众多支持单点登录的 App 没有正确部署 OAuth2.0 认证协议，攻击者可利用此漏洞远程登陆任何用户的 App 账户，泄露用户敏感信息，或者以用户名义在相应 App 上操作。OAuth2.0 部署问题其实是个基础性的错误。但是，影响范围却可能很严重。攻击者如果黑入旅游 App，可以获得用户的完整行程信息；如果黑的是酒店预订 App，可以预定房间并让受害用户支付；攻击者也有可能盗取地址、银行账户等个人信息。

参考链接：http://www.freebuf.com/news/119308.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