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 29 日-2016 年 09 月 04 日　　2016 年第 36 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 298 个，其中高危漏洞 132 个、中危漏洞 150 个、低危漏洞 16 个。漏洞平均分值为 6.41。本周收录的漏洞中，涉及 0day 漏洞 162 个（占 54%）。其中互联网上出现“ZKTeco ZKBioSecurity 3.0 硬编码证书远程系统命令执行漏洞”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 1107 个，与上周（1624 个）环比下降 32%。

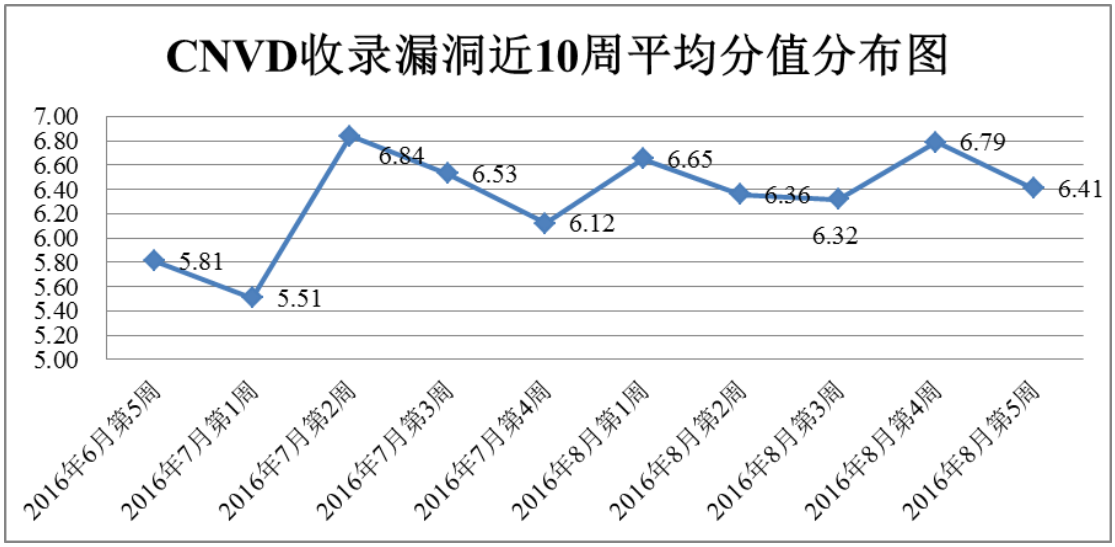

图 1 CNVD 收录漏洞近 10 周平均分值分布图

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 298 个漏洞。报送情况如表 1 所示。其中，恒安嘉新、绿盟科技、天融信、安天实验室等单位报送数量较多。奇虎（补天平台）、漏洞盒子、西安四叶草信息技术有限公司、新疆天山智汇信息科技有限公司、广州神月信息安全技术有限公司、江苏君立华域信息安

全技术有限公司、中国航天科工四院软件评测中心及其他个人白帽子向 CNVD 提交了 1107 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）	998	998
恒安嘉新	134	0
绿盟科技	129	0
天融信	109	0
安天实验室	87	0
东软	68	1
H3C	47	0
启明星辰	43	4
中国电信集团系统集成有限责任公司	39	0
杭州安恒信息技术有限公司	34	0
漏洞盒子	22	22
西安四叶草信息技术有限公司	19	19
新疆天山智汇信息科技有限公司	17	17
广州神月信息安全技术有限公司	4	4
江苏君立华域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	2	2
CNCERT 天津分中心	11	11
个人	25	25
报送总计	1792	1107
录入总计	298（去重）	1107

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 298 个漏洞。其中应用程序漏洞 146 个，web 应用漏洞 119 个，网络设备漏洞 17 个，安全产品 9 个，操作系统漏洞 7 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	146
web 应用漏洞	119
网络设备漏洞	17
安全产品漏洞	9
操作系统漏洞	7

表 2 漏洞按影响类型统计表

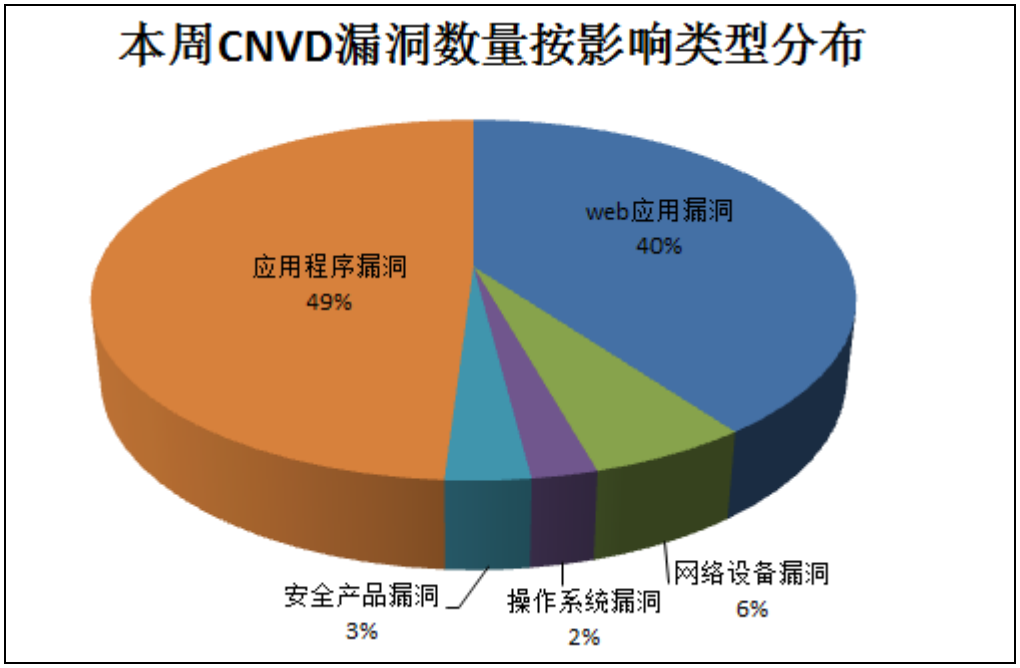

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 PHP、Cisco、Foxit 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	PHP	21	7%
2	Cisco	13	4%
3	Foxit	13	4%
4	SAP	8	3%
5	Red Hat	7	2%
6	TYPO3	6	2%

7	IBM	6	2%
8	WordPress	5	2%
9	OwnCloud	5	2%
10	其他	214	72%

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 8 个电信行业漏洞，2 个移动互联网行业漏洞（如下图所示）。其中，“Qualcomm Innovation Center Android contributions for MSM 整数溢出漏洞”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/

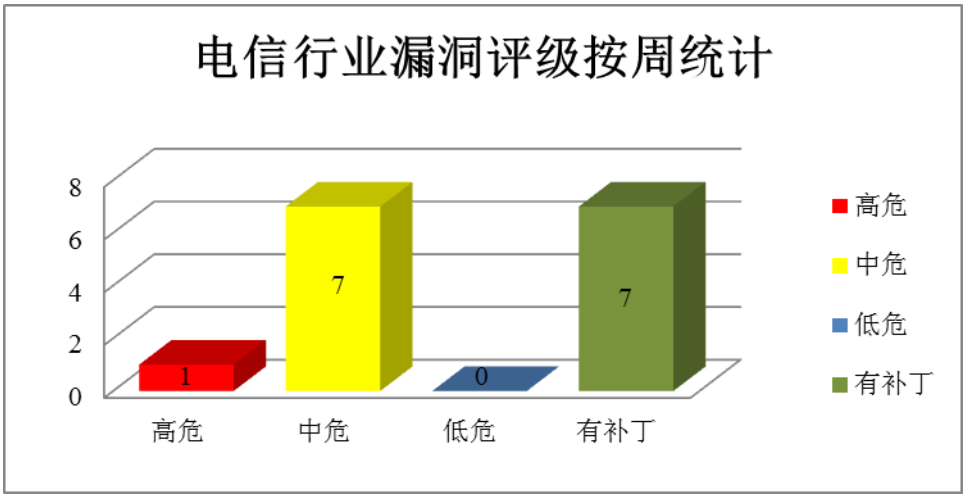

图 3 电信行业漏洞统计

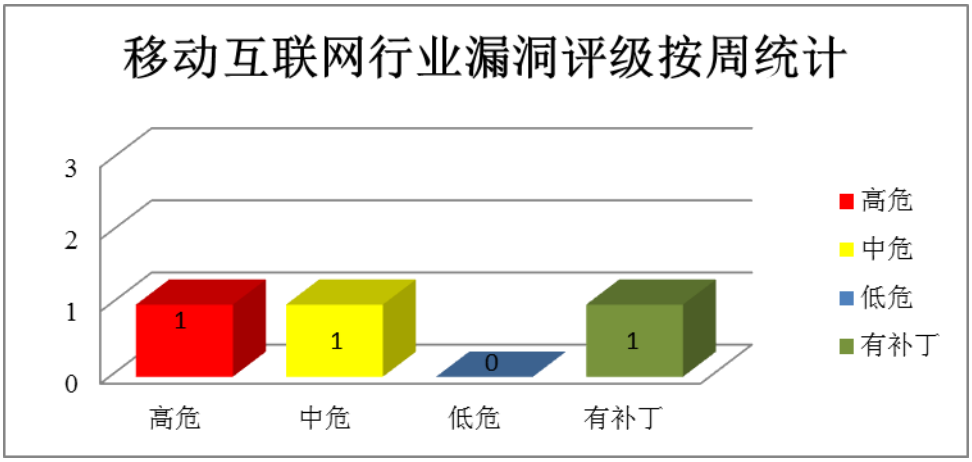

图 4 移动互联网行业漏洞统计

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、PHP 产品安全漏洞

PHP 是一种开源的通用计算机脚本语言。本周，该产品被披露存在信息泄露和拒绝服务漏洞，攻击者可利用漏洞泄露敏感信息和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：PHP 'ext/sqlite3/sqlite3.c'存在多个拒绝服务漏洞、PHP 'zend_virtual_cwd()'函数空指针引用拒绝服务漏洞、PHP 'ext/standard/string.c'信息泄露漏洞、PHP 'xp_socket.c'拒绝服务漏洞、PHP 'pgsql_statement.c'拒绝服务漏洞、PHP 'ext/readline/readline.c'拒绝服务漏洞、PHP 'gd/libgd/gd_gif_out.c'信息泄露漏洞、PHP 'interface.c'拒绝服务漏洞等。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-2016-07124
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07127
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07125
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06919
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06920
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06921
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06928
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06929

2、Cisco 产品安全漏洞

Cisco WebEx Meetings 是网络会议解决方案。Cisco Small Business 220 Series Smart Plus Switches 是一款智能交换机。Cisco Wireless LAN Controller 是一款思科无线局域网控制器。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行远程代码、获取未授权访问限制或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Cisco Wireless LAN Controller 拒绝服务漏洞（CNVD-2016-07077）、Cisco Wireless LAN Controller TSM SNMP 拒绝服务漏洞、Cisco WebEx Meetings Player 远程代码执行漏洞、Cisco WebEx Meetings Player 拒绝服务漏洞、Cisco Small Business 220 Series Smart Plus Switches 未授权访问漏洞、Cisco Small Business 220 Series Smart Plus Switches 跨站请求伪造漏洞、Cisco Small Business 220 Series Smart Plus Switches 跨站脚本漏洞、Cisco Small Business 220 Series Smart Plus Switches 拒绝服务漏洞等。其中，“Cisco WebEx Meetings Player 远程代码执行漏洞”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-2016-07077
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07020

http://www.cnvd.org.cn/flaw/show/CNVD-2016-07018
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07019
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07070
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07071
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07068
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07072

3、Foxit 产品安全漏洞

Foxit Reader 是中国福昕（Foxit）软件公司的出品的一款小型的 PDF 文档查看和打印程序，PhantomPDF 是一个商业版。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞远程获取敏感信息，执行任意代码或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Foxit Reader 和 PhantomPDF 远程命令执行漏洞（CNVD-2016-07030）、Foxit Reader and Foxit PhantomPDF 存在多个拒绝服务漏洞、Foxit Reader and PhantomPDF DLL 加载远程命令执行漏洞、Foxit Reader and Foxit PhantomPDF 存在多个远程命令执行漏洞、Foxit Reader and Foxit PhantomPDF 越界读信息泄露漏洞、Foxit Reader and Foxit PhantomPDF 越界读写远程命令执行漏洞、Foxit Reader 和 PhantomPDF 远程命令执行漏洞、Foxit Reader 'ConvertToPDF'插件信息泄露漏洞等。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-2016-07030
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07031
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07029
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07028
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07027
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07026
http://www.cnvd.org.cn/flaw/show/CNVD-2016-07025
http://www.cnvd.org.cn/flaw/show/CNVD-2016-06930

4、SAP 产品安全漏洞

SAP TREX 是德国思爱普（SAP）公司的一款用于 SAP NetWeaver 集成技术平台中的搜索引擎。SAP Utility Customer E-Services 是一个基于 j2ee 的 Web 应用程序。SAP HANA 是一套高性能的实时数据分析平台。SAP Solution Manager 是一套集系统监控、SAP 支持桌面、自助服务、ASAP 实施等多个功能为一体的系统管理平台。SAP NetWeaver 是一套面向服务的集成化应用平台，SAP NetWeaver AS Java 是一款运行于 NetWeaver 中且基于 Java 编程语言的应用服务器。SAP Adaptive Server Enterprise（Sybase ASE）是一套关系型数据库管理系统。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、远程执行命令或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：SAP TREX 信息泄露漏洞、SAP TREX 远程命令执行漏洞、SAP Utility Customer E-Services 点击劫持漏洞、SAP HANA Enterprise 安全绕过漏洞、SAP Solution Manager 远程命令注入漏洞、SAP NetWeaver SAPSTARTSRV 远程缓冲区溢出漏洞、SAP NetWeaver AS JAVA 拒绝服务漏洞、SAP Adaptive Server Enterprise 拒绝服务漏洞。其中，“SAP TREX 远程命令执行漏洞、SAP Solution Manager 远程命令注入漏洞”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-2016-07151

http://www.cnvd.org.cn/flaw/show/CNVD-2016-07152

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06874

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06865

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06875

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06864

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06863

http://www.cnvd.org.cn/flaw/show/CNVD-2016-06862

5、ZKTeco ZKBioSecurity 3.0 硬编码证书远程系统命令执行漏洞

ZKBioSecurity 是一个生物识别安防综合管理平台。本周，ZKBioSecurity 被披露存在远程系统命令执行漏洞。攻击者可利用 JSP 应用程序恶意 WAR 归档文件上传，导致攻击者以系统权限执行任意代码的能力。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-2016-07101

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-2016-06966	OwnCloud Gallery Application HTML 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：https://owncloud.org/
CNVD-2016-07014	vBulletin forumrunner/includes/moderation.php SQL 注入漏洞	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.vbulletin.org/forum/showthread.php?t=322848
CNVD-2016-07018	Cisco WebEx Meetings Player 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，补丁获取链接：http://tools.cisco.com/security/center/

			content/CiscoSecurityAdvisory/cisco-sa-20160831-meetings-player
CNVD-2016-07034	NMAP DLL 加载本地命令执行漏洞	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：http://seclists.org/nmap-dev/2016/q3/63
CNVD-2016-07081	IBM Tivoli Storage Manager for Virtual Environments 安全绕过漏洞	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：http://www-01.ibm.com/support/docview.wss?uid=swg21988781
CNVD-2016-07088	MAC-Telnet 'mactelnet.c'缓冲区溢出漏洞	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/haakonnessjoen/MAC-Telnet/pull/20
CNVD-2016-07087	Qualcomm Innovation Center Android contributions for MSM 整数溢出漏洞	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：https://www.kernel.org/
CNVD-2016-07086	Qualcomm Innovation Center Android contributions for MSM 缓冲区溢出漏洞	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：https://www.kernel.org/
CNVD-2016-07120	Red Hat JBoss Operations Network 远程权限提升漏洞	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://rhn.redhat.com/errata/RHSA-2016-1785.html
CNVD-2016-07119	ImageMagick 拒绝服务漏洞	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.imagemagick.org/script/index.php

表 4 部分重要高危漏洞列表

小结：本周，PHP 产品被披露存在信息泄露和拒绝服务漏洞，攻击者可利用漏洞泄露敏感信息和发起拒绝服务攻击。此外，Cisco、Foxit、SAP 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞远程执行任意代码、泄露敏感信息或发起拒绝服务攻击等。另外，ZKBioSecurity 被披露存在远程系统命令执行漏洞。攻击者可利用 JSP 应用程序恶意 WAR 归档文件上传，导致攻击者以系统权限执行任意代码的能力。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. Linux netfilter OOB root 提权漏洞分析

著名的 ExploitDatabase 网站最近贴出了一个 netfilter 模块的提权 POC。该漏洞是内核 netfilter 处理 setsockopt 相关代码（check_compat_entry_size_and_hooks 和 check_entry 函数）在处理应用层传下来的数据时审查不严格，处理逻辑也存在缺陷，使内核在调用 module_put 函数时操作了应用层传下来的地址，导致内核直接对应用层输入的地址执行减一操作，相当于是内核任意地址写漏洞。

参考链接：http://www.freebuf.com/vuls/112969.html

2. 链接地址中的 target=”_blank”属性，为钓鱼攻击打开了大门

现在，许多主流的互联网服务提供商都会在网页的链接地址中加入 target=”_blank”属性，而这绝对是一种非常不安全的行为。不仅如此，target=”_blank”属性还将会使广大互联网用户暴露在钓鱼攻击的风险之下。当用户点击了某个网站中带有 target=”_blank”属性的超链接后，浏览器会单独新建一个标签页来显示该链接所指向的内容。但是请注意，在这一瞬间，浏览器会允许新建的标签页通过一个名为“window.opener”的浏览器 API 来与之前的网页进行短暂通信。此时，攻击者就可以将恶意代码嵌入在新打开的网站中，然后检测用户是从哪一个网站跳转过来的，最后再利用 window.opener 接口来迫使原始网页打开一个新的 URL 地址。Instagram、Facebook、以及 Twitter 等大型社交网站都会受到这种攻击的影响。修复该问题最简单的方法就是在网站所有的链接中加入 rel=”noopener”属性。

参考链接：http://www.freebuf.com/vuls/113634.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