

信息安全漏洞周报

2017 年 02 月 13 日-2017 年 02 月 19 日

2017 年第 8 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 254 个，其中高危漏洞 106 个、中危漏洞 127 个、低危漏洞 21 个。漏洞平均分为 6.13。本周收录的漏洞中，涉及 0day 漏洞 57 个（占 22%）。其中互联网上出现“OIC Exponent CMS SQL 注入漏洞（CNVD-2017-01280）、NewsBee CMS SQL 注入漏洞”等零日代码攻击漏洞，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 761 个，与上周（773 个）环比持平。

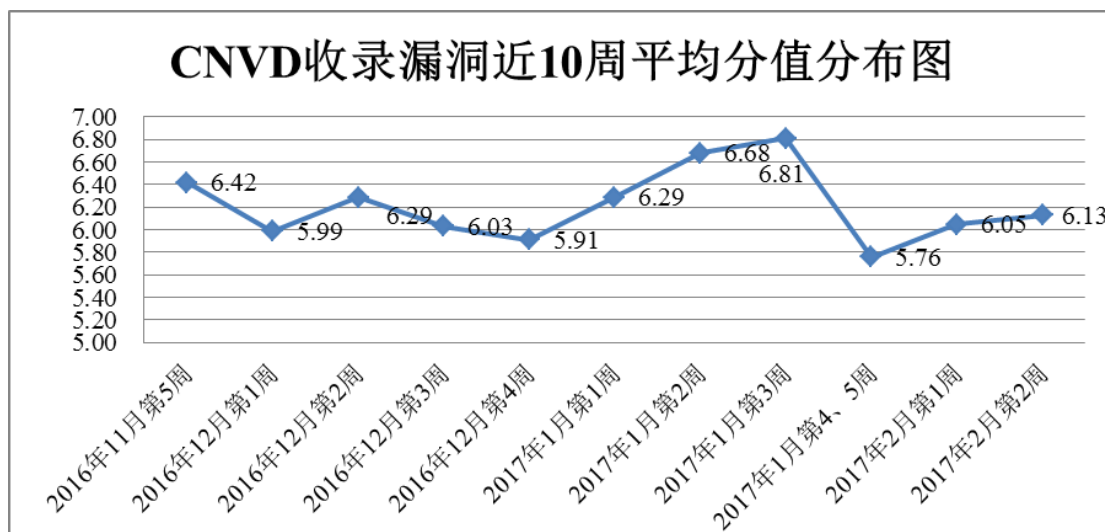


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 16 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 254 个漏洞。报送情况如表 1 所示。其中，安天实验室、蓝盾信息技术有限公司、启明星辰、天融信等单位报送数量较多。360 网神、漏洞盒子、广西鑫瀚科技有限公司、广州市网迅信息技术有限公司及其他个人白帽子向 CNVD 提交了 761 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	526	526
安天实验室	213	0
蓝盾信息安全技术有限公司	148	1
启明星辰	103	0
天融信	94	0
华为技术有限公司	91	0
H3C	83	0
绿盟科技	49	0
中国电信集团系统集成有限责任公司	30	0
恒安嘉新	24	0
安全狗	12	0
杭州安恒信息技术有限公司	9	0
北京数字观星科技有限公司	9	0
深圳市深信服电子科技有限公司	7	7
西安四叶草信息技术有限公司	3	3
南京铨迅信息技术股份有限公司	3	3
漏洞盒子	136	136
广西鑫瀚科技有限公司	13	13
广州市网迅信息技术有限公司	1	1
CNCERT 吉林分中心	11	11
CNCERT 海南分中心	4	4

CNCERT 江西分中心	3	3
CNCERT 湖南分中心	2	2
CNCERT 上海分中心	3	3
CNCERT 陕西分中心	2	2
CNCERT 广东分中心	1	1
个人	45	45
报送总计	1625	761
录入总计	254（去重）	761

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 254 个漏洞。其中应用程序漏洞 159 个，web 应用漏洞 45 个，操作系统漏洞 41 个，网络设备漏洞 7 个，安全产品漏洞 1 个,数据库漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	159
web 应用漏洞	45
操作系统漏洞	41
网络设备漏洞	7
安全产品漏洞	1
数据库漏洞	1

表 2 漏洞按影响类型统计表

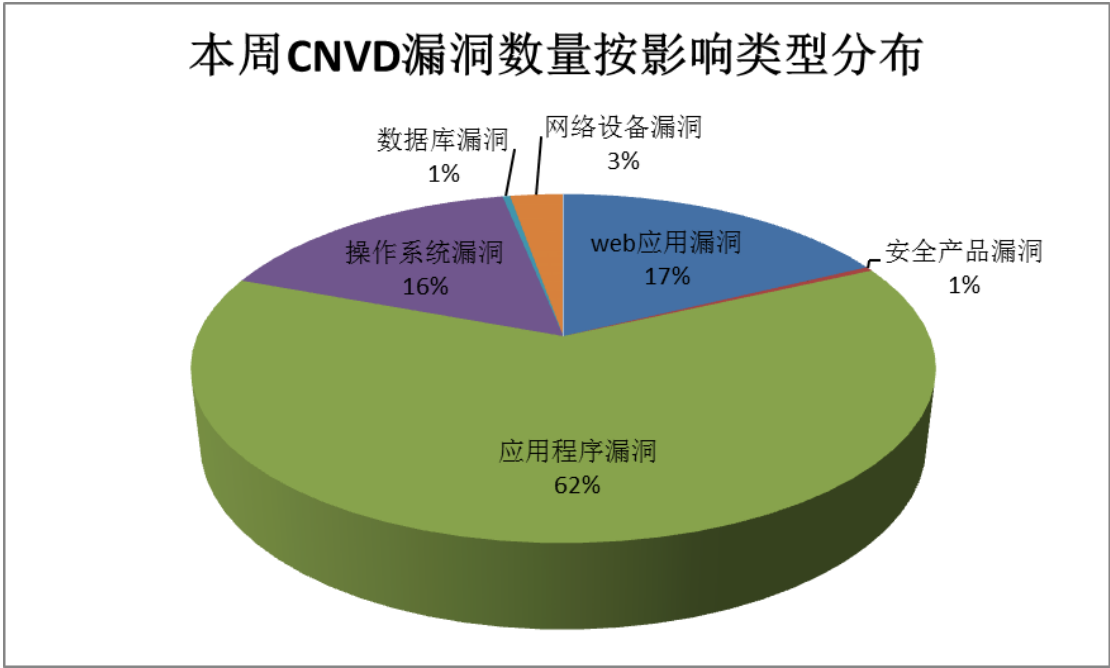


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Google、IBM、Joomla 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	Google	41	16%
2	IBM	34	13%
3	Joomla	18	7%
4	GStreamer	14	6%
5	CloudBees	10	4%
6	Cisco	5	2%
7	Libgd	5	2%
8	DuomiCms	4	2%
9	Huawei	4	2%
10	其他	119	46%

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 2 个电信行业漏洞，42 个移动互联网行业漏洞，3 个工控系统行业漏洞（如下图所示）。其中，“Ecava IntegraXor 存在多个 SQL 注入漏洞、SIEMENS SIMATIC Logon 认证绕过漏洞、Google Android 内核文件子系统权限提升漏洞、Go

Google Android Surfaceflinger 远程代码执行漏洞、Google Android MediaTek driver 权限提升漏洞、Google Android Qualcomm crypto driver 代码执行漏洞、Google Pixel/Pixel XL HTC 触屏驱动器权限提升漏洞、Google Android Kernel Networking Subsystem 远程权限提升漏洞”等漏洞的综合评级为“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/>

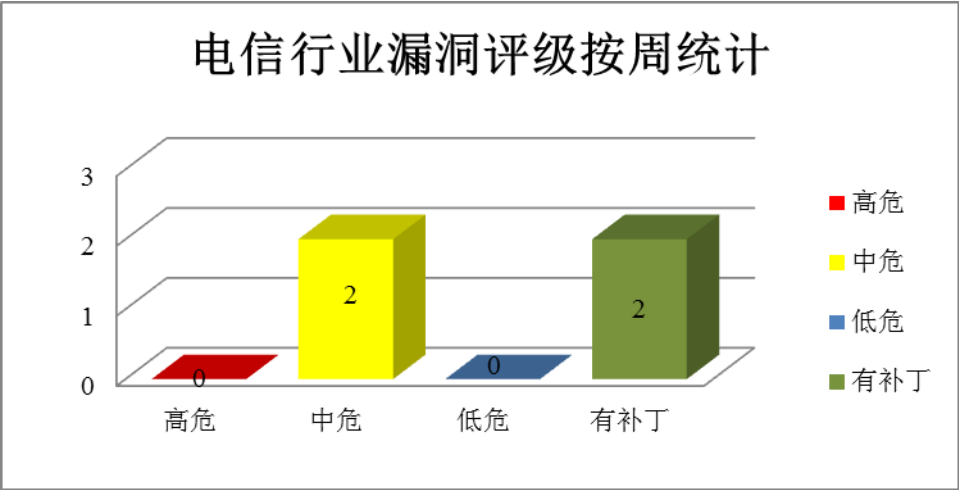


图 3 电信行业漏洞统计

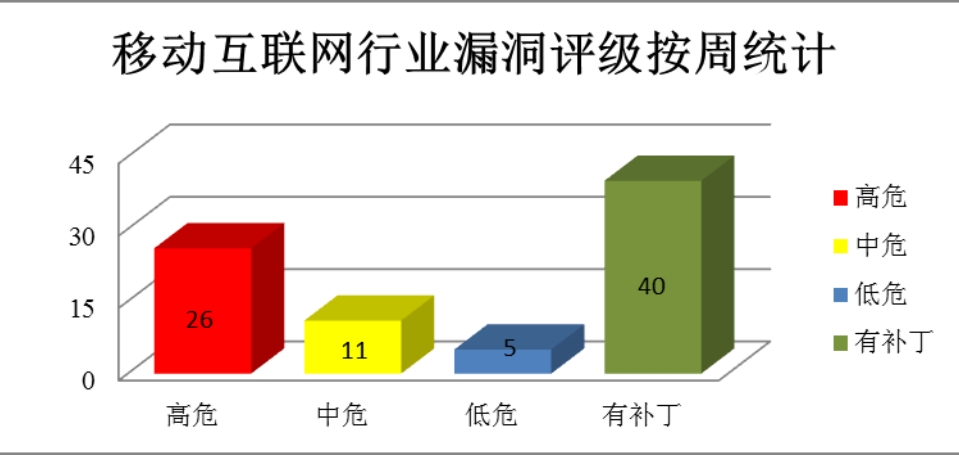


图 4 移动互联网行业漏洞统计

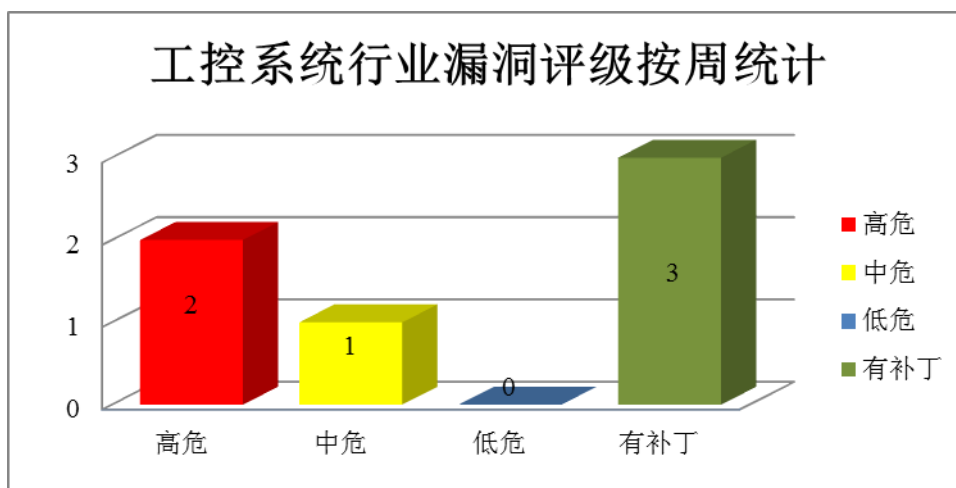


图 5 工控系统行业漏洞统计

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、Google 产品安全漏洞

Android 是美国谷歌公司和开放手持设备联盟共同开发的一套以 Linux 为基础的开源操作系统。本周，该产品被披露存在权限提升漏洞，攻击者可利用漏洞以提升的权限执行任意代码。

CNVD 收录的相关漏洞包括：Google Android Qualcomm Wi-Fi driver 权限提升漏洞（CNVD-2017-01426、CNVD-2017-01395、CNVD-2017-01396、CNVD-2017-01397）、Google Android Audioserver 权限提升漏洞（CNVD-2017-01452、CNVD-2017-01453、CNVD-2017-01454、CNVD-2017-01455）。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-2017-01426>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01395>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01396>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01397>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01452>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01453>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01454>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01455>

2、IBM 存在产品安全漏洞

IBM Security Access Manager 是美国 IBM 公司的一款安全访问管理器。本周，该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、注入任意代码或发起跨站

脚本攻击等。

CNVD 收录的相关漏洞包括：IBM Security Access Manager 信息泄露漏洞（CNVD-2017-01413、CNVD-2017-01412、CNVD-2017-01305、CNVD-2017-01307）、IBM Security Access Manager 任意代码注入漏洞、IBM Security Access Manager 跨站请求伪造漏洞（CNVD-2017-01308）、IBM Security Access Manager XML 外部注入漏洞、IBM AIX 本地权限提升漏洞（CNVD-2017-01334），其中，“IBM Security Access Manager XML 外部注入漏洞、IBM AIX 本地权限提升漏洞（CNVD-2017-01334）”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-2017-01413>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01412>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01305>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01307>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01304>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01308>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01306>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01334>

3、Joomla 产品多款组件安全漏洞

Joomla 是一款开放源码的内容管理系统(CMS)。本周，上述产品被披露存在 SQL 注入漏洞，攻击者可利用漏洞访问或修改数据库数据。

CNVD 收录的相关漏洞包括：Joomla JE Tour 组件 SQL 注入漏洞、Joomla JE auction 组件 SQL 注入漏洞、Joomla Hbooking 组件 SQL 注入漏洞、Joomla JE Quiz 组件 SQL 注入漏洞、Joomla JE Auto 组件 SQL 注入漏洞、Joomla Soccer Bet 组件 SQL 注入漏洞、Joomla onisQuotes 组件 SQL 注入漏洞、Joomla onisMusic 组件 SQL 注入漏洞。上述漏洞的综合评级为“高危”。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-2017-01465>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01466>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01467>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01468>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01472>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01474>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01479>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01480>

4、GStreamer 产品安全漏洞

GStreamer 是一个开源的多媒体框架。本周，该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：GStreamer gst_avi_demux_parse_ncdt 函数拒绝服务漏洞、GStreamer gst_riff_create_audio_caps 函数拒绝服务漏洞、GStreamer gst-plugins-good 拒绝服务漏洞（CNVD-2017-01450、CNVD-2017-01451、CNVD-2017-01486）、GStreamer gst-plugins-base 拒绝服务漏洞、GStreamer 拒绝服务漏洞（CNVD-2017-01488）、GStreamer gst-plugins-good 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-2017-01572>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01573>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01450>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01451>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01487>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01488>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01485>
<http://www.cnvd.org.cn/flaw/show/CNVD-2017-01486>

5、Cisco Adaptive Security Appliance CX Context-Aware Security 拒绝服务漏洞

Cisco Adaptive Security Appliance CX Context-Aware Security 是美国思科(Cisco)公司的一款用于扩展 ASA 平台的附加服务模块。本周，Cisco 被披露存在拒绝服务漏洞。攻击者可利用漏洞造成拒绝服务。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-2017-01330>

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-2017-01269	Spice 缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://bugzilla.redhat.com/show_bug.cgi?id=1401603
CNVD-2017-01319	Vivint SkyControl Panel 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，详情请关注厂商主页： http://www.vivint.com/en/
CNVD-2017-01365	Wordpress 4.7.0/4.7.1 内容注入漏洞	高	用户可联系供应商获得补丁信息： https://wordpress.org/
CNVD-2017-01404	Tor Browser Launcher 中间人攻击漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			https://github.com/micahflee/torbrowser-launcher/issues/229
CNVD-2017-01482	FFmpeg 堆栈缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序, 请及时关注更新: http://seclists.org/oss-sec/2017/q1/276
CNVD-2017-01523	libevent 拒绝服务漏洞	高	用户可联系供应商获得补丁信息: http://libevent.org/
CNVD-2017-01524	libevent 拒绝服务漏洞 (CNVD-2017-01524)	高	用户可联系供应商获得补丁信息: http://libevent.org/
CNVD-2017-01525	libevent 拒绝服务漏洞 (CNVD-2017-01525)	高	用户可联系供应商获得补丁信息: http://libevent.org/
CNVD-2017-01528	libGD 缓冲区下溢漏洞	高	用户可联系供应商获得补丁信息: https://github.com/libgd/libgd/
CNVD-2017-01530	libGD 'gd_gd2.c'整数溢出漏洞	高	用户可联系供应商获得补丁信息: https://github.com/libgd/libgd/

表 4 部分重要高危漏洞列表

小结: 本周, Google 被披露存在权限提升漏洞, 攻击者可利用漏洞以提升的权限执行任意代码。此外, IBM、Joomla、GStreamer 等多款产品被披露存在多个漏洞, 攻击者利用漏洞可泄露敏感信息、注入任意代码或发起拒绝服务攻击等。另外, Cisco 被披露存在拒绝服务漏洞。攻击者可利用漏洞造成拒绝服务。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. 暴风影音 AviIndexChunk 字段堆溢出漏洞

暴风影音 AviIndexChunk 字段存在堆溢出漏洞。在页堆申请时, 只是单纯地将页堆大小设置为 cbFileSize 的 2 倍, 没有考虑页堆前 8 个字节要写入固定的内容 IndexChunk Header, 从而造成了堆溢出。在暴风影音进程内部, 多次打开 poc.avi 样本会导致之前被溢出的低碎片堆被释放掉。由于没添加相关 try catch 异常处理策略, 最终会导致进程的崩溃。

参考链接: <http://www.freebuf.com/vuls/126892.html>

2. 美国一大学遭到 5000 余台校园物联网设备 DDoS 攻击

国一大学校园网遭到 DDoS 攻击, 大批学生表示网速慢成狗。经校方人员调查后发现, 发起 DDoS 攻击的正是校园周围 5000 多台 IoT (物联网) 设备构成的僵尸网络。在这些受感染 IoT 设备中, 大多是校园内的自动售货机。建议企业应该密切地关注 IoT 设备的网络设置, 并尽可能将其与互联网和其他设备的访问分开。还建议将物联网设备与常规 IT 资产清单一起使用, 并使用基本安全措施, 比如更改默认凭据和轮换强大的 Wi-Fi 网络密码。

参考链接: <http://www.freebuf.com/news/127052.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