国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2015 年 12 月 07 日-2015 年 12 月 13 日 **2015 年第 50 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 128 个，其中高危漏洞 65 个、中危漏洞 59 个、低危漏洞 4 个。上述漏洞中，可利用来实施远程攻击的漏洞有 114 个。本周收录的漏洞中，已有 126 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。其中互联网上出现“OpenLDAP 弱密码漏洞”零日漏洞，请使用相关产品的用户注意加强防范。

本周，互联网上披露了此前 Java 反序列化远程代码执行漏洞相关的利用工具（带 UI），主要针对 JBoss（实现远程代码执行）和 Weblogic（需反弹）两类容器。CNVD 接收并处置了数十起与政府和重要行业单位相关的漏洞事件案例，预计针对该漏洞的攻击案例在近期将会持续。

成员单位报送漏洞统计

本周，共 7 家成员单位、合作伙伴及个人报送了本周收录的全部 128 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、启明星辰、天融信、恒安嘉新等单位报送数量较多。补天平台、乌云、漏洞盒子及白帽子向 CNVD 提交了 1114 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)	663	663
启明星辰	284	0
天融信	123	0
恒安嘉新	120	0

安天实验室	117	0
绿盟科技	101	0
H3C	2	0
乌云	412	412
漏洞盒子	24	24
High-Tech Bridge Security Research Lab	2	2
CNCERT 宁夏分中心	1	1
个人	12	12
报送总计	1861	1114
录入总计	128（去重）	1114

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Google、Microsoft、Autodesk 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	Google	47	37%
2	Microsoft	38	30%
3	Autodesk	6	5%
4	Cisco	6	5%
5	OpenSSL	5	3%
6	Red Hat	2	2%
7	Sensio Labs	2	2%
8	Ubuntu	2	2%
9	Blue Coat Systems, Inc	2	2%
10	其他	18	12%

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 128 个漏洞。其中应用程序漏洞 87 个，操作系统漏洞 31 个，

Web 应用漏洞 5 个，网络设备漏洞 4 个，安全产品漏洞 1 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	87
操作系统漏洞	31
Web 应用漏洞	5
网络设备漏洞	4
安全产品漏洞	1

表 3 漏洞按影响类型统计表

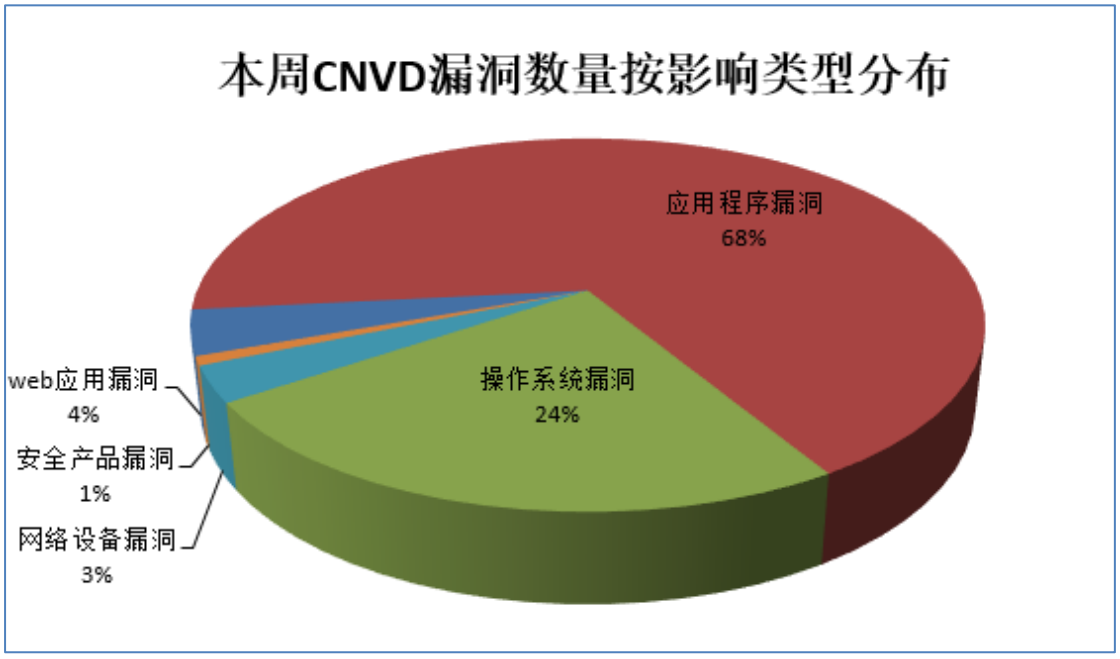

图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 2 个电信行业漏洞、20 个移动互联网行业漏洞、1 个工控系统行业漏洞（如下图表所示）。其中，“Android mediaserver 内存破坏漏洞、Android mediaserver 内存破坏漏洞（CNVD-2015-08006、CNVD-2015-08005、CNVD-2015-08037）、Android 显示驱动程序内存破坏漏洞（CNVD-2015-08004）、Android 显示驱动程序内存破坏漏洞、Android SystemUI 权限提升漏洞、Android System Server 信息泄露漏洞（CNVD-2015-08051）、Android Wi-Fi 权限提升漏洞、Android Skia 内存破坏漏洞、Android libstagefright 权限提升漏洞、Android kernel 权限提升漏洞”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-2015-07940	Cisco Nexus 5000 Series NX-OS USB 驱动输入验证本地拒绝服务漏洞	中	是
电信	CNVD-2015-07984	Blue Coat Systems ProxySG SGOS 信息	中	是

		泄露漏洞		
移动互联网	CNVD-2015-08006	Android mediaserver 内存破坏漏洞（CNVD-2015-08006）	高	是
移动互联网	CNVD-2015-08005	Android mediaserver 内存破坏漏洞（CNVD-2015-08005）	高	是
移动互联网	CNVD-2015-08004	Android 显示驱动程序内存破坏漏洞（CNVD-2015-08004）	高	是
移动互联网	CNVD-2015-08003	Android 显示驱动程序内存破坏漏洞	高	是
移动互联网	CNVD-2015-08002	Android mediaserver 内存破坏漏洞	高	是
移动互联网	CNVD-2015-08037	Android mediaserver 内存破坏漏洞（CNVD-2015-08037）	高	是
移动互联网	CNVD-2015-08045	Android SystemUI 权限提升漏洞	高	是
移动互联网	CNVD-2015-08048	Android libstagefright 信息泄露漏洞	中	是
移动互联网	CNVD-2015-08051	Android System Server 信息泄露漏洞（CNVD-2015-08051）	高	是
移动互联网	CNVD-2015-08050	Android Wi-Fi 权限提升漏洞	高	是
移动互联网	CNVD-2015-08049	Android Skia 内存破坏漏洞	高	是
移动互联网	CNVD-2015-08053	Android libstagefright 权限提升漏洞	高	是
移动互联网	CNVD-2015-08052	Android System Server 信息泄露漏洞	中	是
移动互联网	CNVD-2015-08056	Android Media Framework 信息泄露漏洞	中	是
移动互联网	CNVD-2015-08055	Android Audio 组件信息泄露漏洞	低	是
移动互联网	CNVD-2015-08054	Android libstagefright 信息泄露漏洞（CNVD-2015-08054）	中	是
移动互联网	CNVD-2015-08057	Android Wi-Fi 信息泄露漏洞	中	是
移动互联网	CNVD-2015-08059	Android SystemUI 信息泄露漏洞	中	是
移动互联网	CNVD-2015-08058	Android kernel 权限提升漏洞	高	是
移动互联网	CNVD-2015-08060	Android Native Frameworks Library 信息泄露漏洞	中	是
工控系统	CNVD-2015-07953	Siemens APOGEE Insight Database Conversion Tool DLL 劫持漏洞	高	否

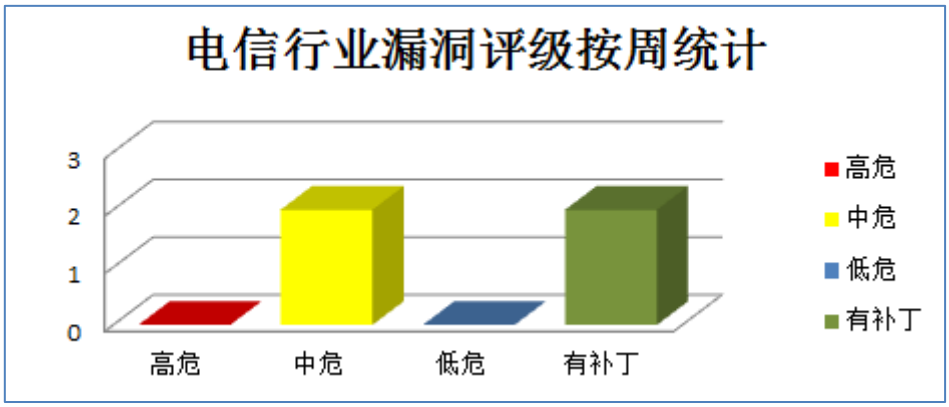

图 1 电信行业漏洞统计

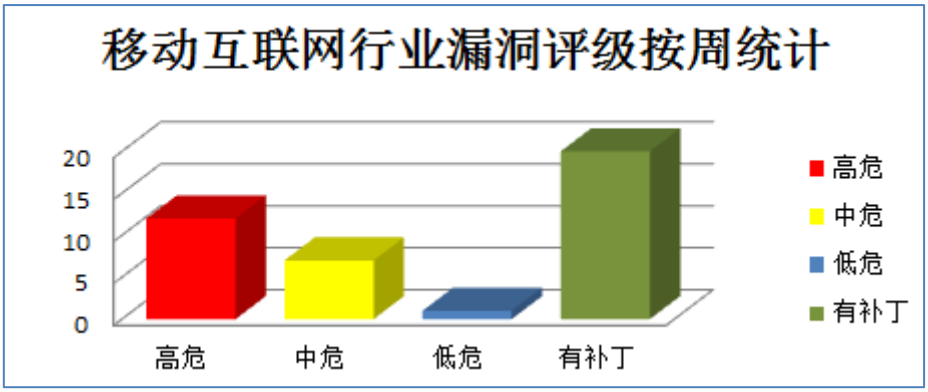

图 2 移动互联网行业漏洞统计

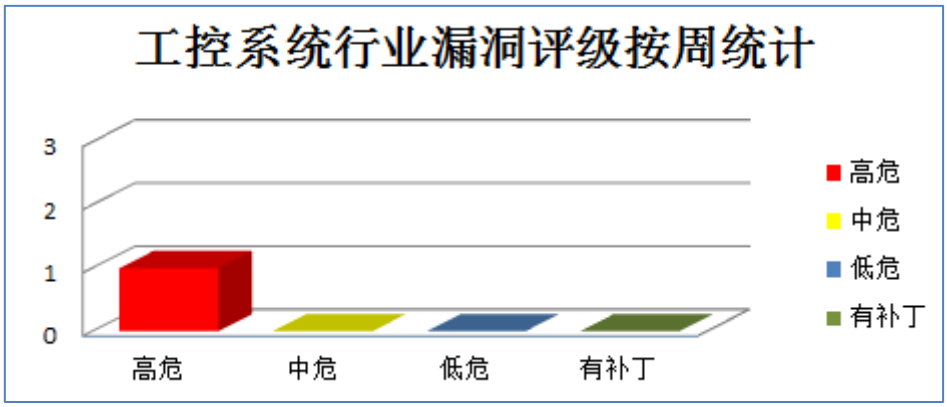

图 3 工控系统行业漏洞统计

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、 Microsoft 产品安全漏洞

12 月 8 日，微软发布了 2015 年 12 月份的月度例行安全公告，共含 12 项更新，修复了 MicrosoftWindows、Internet Explorer、Edge、.NET Framework、Office、Skype for Business、Lync 和 Silverlight 中存在的 71 个安全漏洞。其中，8 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 收录的相关漏洞包括：Microsoft Internet Explorer 内存破坏漏洞（CNVD-2015-08061、CNVD-2015-08067、CNVD-2015-08066、CNVD-2015-08065、CNVD-2015-08064、CNVD-2015-08063、CNVD-2015-08062、CNVD-2015-08070）。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/3753

2、 Google 产品安全漏洞

Google Chrome 是美国谷歌（Google）公司开发的一款 Web 浏览器。本周，上述产

品被披露存在内存错误引用和拒绝服务漏洞。攻击者利用漏洞可执行任意代码和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Google Chrome 内存错误引用漏洞（CNVD-2015-07955）、Google Chrome AppCache 内存错误引用漏洞（CNVD-2015-07956）、Google Chrome AppCache 内存错误引用漏洞、Google Chrome Skia 拒绝服务漏洞（CNVD-2015-07963）、Google Chrome Extensions 内存错误引用漏洞、Google Chrome Infobars 内存错误引用漏洞、Google Chrome 'ContainerNode::notifyNodeInsertedInternal'内存错误引用漏洞、Google Chrome 拒绝服务漏洞（CNVD-2015-07978）。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-2015-07955
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07956
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07957
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07963
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07964
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07967
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07979
http://www.cnvd.org.cn/flaw/show/CNVD-2015-07978

3、 Autodesk 产品安全漏洞

Autodesk Design Review 是免费 DWF 查看器软件。本周，上述产品被披露存在远程代码执行漏洞。攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括：Autodesk Design Review BMP RLE 远程代码执行漏洞、Autodesk Design Review FLI RLE 远程代码执行漏洞、Autodesk Design Review BMP biClrUsed 远程代码执行漏洞、Autodesk Design Review PCX 远程代码执行漏洞、Autodesk Design Review GIF DataSubBlock 远程代码执行漏洞、Autodesk Design Review GIF GlobalColorTable 远程代码执行漏洞。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-2015-08032
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08033
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08034
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08035
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08036
http://www.cnvd.org.cn/flaw/show/CNVD-2015-08044

4、 Cisco 产品安全漏洞

Cisco Unified Computing System Manager 可对统一计算系统内的所有软硬件组件提

供统一的、嵌入式管理。Cisco Unified SIP Phone 3905 是一款 SIP 电话设备。Cisco NX-OS 软件是一个数据中心级的操作系统,该操作系统体现模块化设计、永续性和可维护性。Cisco Small Business RV 系列路由器可提供虚拟专用网络技术远程。Cisco TelePresence 是思科网真解决方案。本周，上述产品被披露存在跨站脚本、跨站请求伪造、信息泄露和拒绝服务漏洞。攻击者利用漏洞获取敏感信息，执行跨站脚本、跨站请求伪造攻击和发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Cisco UCS Central Software 跨站脚本漏洞、Cisco UCS Central Software 服务器端请求伪造漏洞、Cisco Unified SIP Phone 3905 Series Phones 远程拒绝服务漏洞、Cisco Nexus 5000 Series NX-OS USB 驱动输入验证本地拒绝服务漏洞、Cisco Small Business RV 路由器信息泄露漏洞、Cisco TelePresence Video Communication Server 信息泄露漏洞。其中，“Cisco Small Business RV 路由器信息泄露漏洞、Cisco TelePresence Video Communication Server 信息泄露漏洞”的综合评级为“高”危。目前，厂商已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-2015-08001

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08000

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07941

http://www.cnvd.org.cn/flaw/show/CNVD-2015-07940

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08068

http://www.cnvd.org.cn/flaw/show/CNVD-2015-08069

5、 OpenLDAP 弱密码漏洞

OpenLDAP 是美国 OpenLDAP 基金会的一个轻型目录访问协议（LDAP）的自由和开源实现，它已被包含在 Linux 发行版中。本周，OpenLDAP 被披露存在弱密码漏洞。攻击者可通过发送特制的密码请求使程序使用弱密码。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-2015-07986

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-2015-07939	多款 IBM 产品安全绕过漏洞（CNVD-2015-07939）	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=swg21970797
CNVD-2015-07946	SearchBlox File Exfiltration 拒绝服务漏洞	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.searchblox.com/downloa

			ds
CNVD-2015-07951	OpenSSL 竞争条件拒绝服务漏洞	高	OpenSSL 0.9.8zh, 1.0.0t, 1.0.1q, 1.0.2e 已经修复该漏洞，建议用户修复更新：https://www.openssl.org
CNVD-2015-07987	多款 F5 产品权限获取漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息：https://support.f5.com/kb/en-us/solutions/public/16000/700/sol16728.html
CNVD-2015-07989	LXCFS 权限获取漏洞	高	用户可联系供应商获得补丁信息：https://linuxcontainers.org/
CNVD-2015-07988	LXCFS 权限获取漏洞（CNVD-2015-07988）	高	用户可联系供应商获得补丁信息：https://linuxcontainers.org/
CNVD-2015-08008	Microsoft Edge CAttrArray 越界读远程代码执行漏洞	高	Microsoft 已经为此发布了一个安全公告（MS15-125）以及相应补丁：http://technet.microsoft.com/security/bulletin/MS15-125
CNVD-2015-08022	Microsoft Windows 核心内存特权提升漏洞（CNVD-2015-08022）	高	Microsoft 已经为此发布了一个安全公告（MS15-135）以及相应补丁：http://technet.microsoft.com/security/bulletin/MS15-135
CNVD-2015-08021	Microsoft Windows 核心内存特权提升漏洞（CNVD-2015-08021）	高	Microsoft 已经为此发布了一个安全公告（MS15-135）以及相应补丁：http://technet.microsoft.com/security/bulletin/MS15-135
CNVD-2015-08020	Microsoft Windows 核心内存特权提升漏洞（CNVD-2015-08020）	高	Microsoft 已经为此发布了一个安全公告（MS15-135）以及相应补丁：http://technet.microsoft.com/security/bulletin/MS15-135

表 3 部分高危漏洞列表

小结：本周，微软发布了 2015 年 12 月份的月度例行安全公告，共含 12 项更新，修复了 MicrosoftWindows、Internet Explorer、Edge、.NET Framework、Office、Skype for Business、Lync 和 Silverlight 中存在的 71 个安全漏洞。允许攻击者利用漏洞提升权限，远程执行任意代码。此外，Google、Autodesk、Cisco 多款产品被披露存在多个安全漏洞，攻击者利用漏洞可进行跨站脚本、跨站请求伪造攻击、执行任意代码和发起拒绝服务攻击等。另外，OpenLDAP 被披露存在一个弱密码漏洞，攻击者可通过发送特制的密码请求使程序使用弱密码。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、EMC 修补 NetWorker 产品漏洞

EMC NetWorker 是一款支持磁盘备份、数据复制、连续数据保护和重复数据消除的应用软件。

本周，EMC 修补了上述产品存在的拒绝服务漏洞，避将攻击者利用漏洞提交特殊的请求使 NetWorker 服务停止响应。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/67706

本周要闻速递

1. 三大杀毒软件存严重漏洞，杀软可变黑客工具

enSilo 的安全专家们在众多杀毒软件中发现了一个严重的安全漏洞，黑客利用该漏洞能把杀毒软件变成黑客的攻击工具。研究者发现，杀毒软件在一个可预测的地址中分配了用于读、写和执行权限的内存，而攻击者掌握到这个内存地址后，则可以利用它向目标系统中注入恶意代码并执行它。受影响的杀毒软件包括 AVG、McAfee、卡巴斯基。

参考链接：http://www.freebuf.com/news/89157.html

2. Xboxlive 数字证书私钥泄露，用户或被中间人攻击

微软确认*Xboxlive.com 域名的 SSL/TLS 数字证书私人密钥遭到泄露，可被攻击者用于尝试发动中间人攻击，但私人密钥不能被用于签发其他证书或代码，或假冒其他域名。Xboxlive 证书包含在所有的 windows 支持版本中，影响范围非常广，但微软目前还没有发现利用私人密钥发动攻击的案例。微软正在更新 Certificate Trust list (CTL) 撤销对该证书的信任，希望每个人都能自动收到撤消 Xboxlive SSL 服务器证书的通知。微软公司并没有说明已经有多少人看到过证书，但很不希望密钥已被用于发动攻击。

参考链接：http://www.freebuf.com/news/89125.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