国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 04 月 17 日-2017 年 04 月 23 日 **2017 年第 17 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 491 个，其中高危漏洞 188 个、中危漏洞 260 个、低危漏洞 43 个。漏洞平均分值为 6.25。本周收录的漏洞中，涉及 0day 漏洞 83 个（占 17%），其中互联网上出现“ZyXEL EMG2926 路由器远程命令执行漏洞、EyesOfNetwork 存在未明 SQL 注入漏洞”零日代码攻击漏洞。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 661 个，与上周（597 个）环比增长 11%。

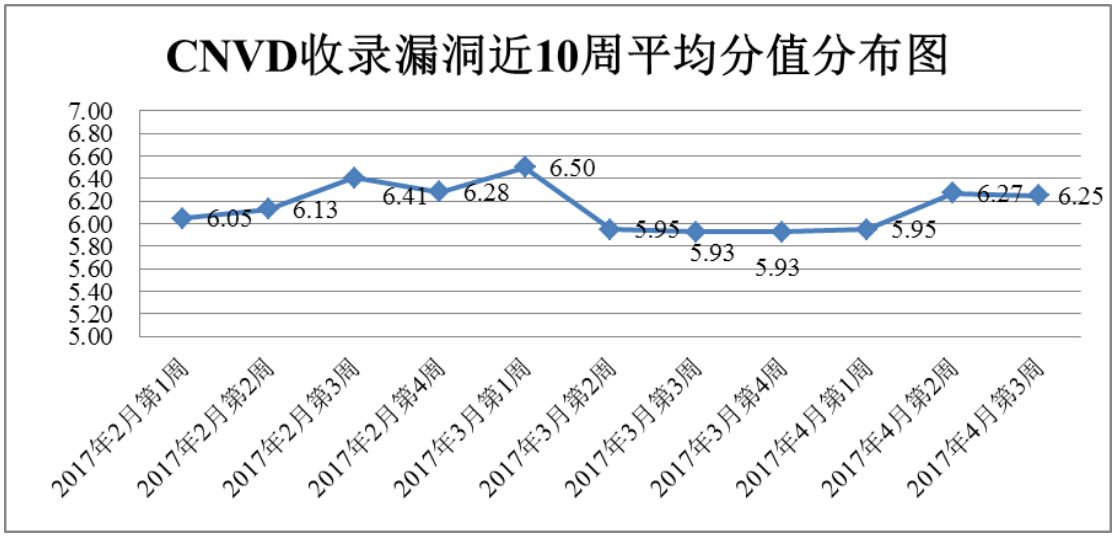

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 15 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 491 个漏洞。报送情况如表 1 所示。其中，华为技术有限公司、绿盟科技、安天实验室、中国电信集团系统集成有限责任公司等单位报送数量较多。北京山石网科信息技术有限公司、杭州朔方信息技术有限公司、山东安云信息技术有限公司、河北网信智安信息技

术有限公司、广西鑫瀚科技有限公司、江苏君立华域信息安全技术有限公司、安徽新华博信息技术股份有限公司、清远职业技术学院及其他个人白帽子向 CNVD 提交了 661 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	348	348
华为技术有限公司	143	0
绿盟科技	100	0
安天实验室	98	0
中国电信集团系统集成有限责任公司	58	0
杭州安恒信息技术有限公司	54	0
H3C	50	1
安全狗	27	3
天融信	21	1
恒安嘉新	17	0
深圳市腾讯计算机系统有限公司（玄武实验室）	17	17
启明星辰	12	12
北京数字观星科技有限公司	5	0
南京铱迅信息技术股份有限公司	1	1
知道创宇	1	1
漏洞盒子	90	90
北京山石网科信息技术有限公司	9	9
杭州朔方信息技术有限公司	4	4
山东安云信息技术有限公司	4	4

河北网信智安信息技术有限公司	3	3
广西鑫瀚科技有限公司	2	2
江苏君立华域信息安全技术有限公司	2	2
安徽新华博信息技术股份有限公司	1	1
清远职业技术学院	1	1
CNCERT 山西分中心	23	23
CNCERT 江西分中心	16	16
CNCERT 新疆分中心	7	7
CNCERT 重庆分中心	7	7
CNCERT 宁夏分中心	6	6
CNCERT 安徽分中心	2	2
CNCERT 河南分中心	2	2
CNCERT 北京分中心	1	1
CNCERT 吉林分中心	1	1
个人	96	96
报送总计	1229	661
录入总计	491（去重）	661

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 491 个漏洞。其中应用程序漏洞 267 个，操作系统漏洞 89 个，web 应用漏洞 76 个，网络设备漏洞 47 个，安全产品漏洞 10 个，数据库漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	267
操作系统漏洞	89
web 应用漏洞	76

网络设备漏洞	47
安全产品漏洞	10
数据库漏洞	2

表 2 漏洞按影响类型统计表

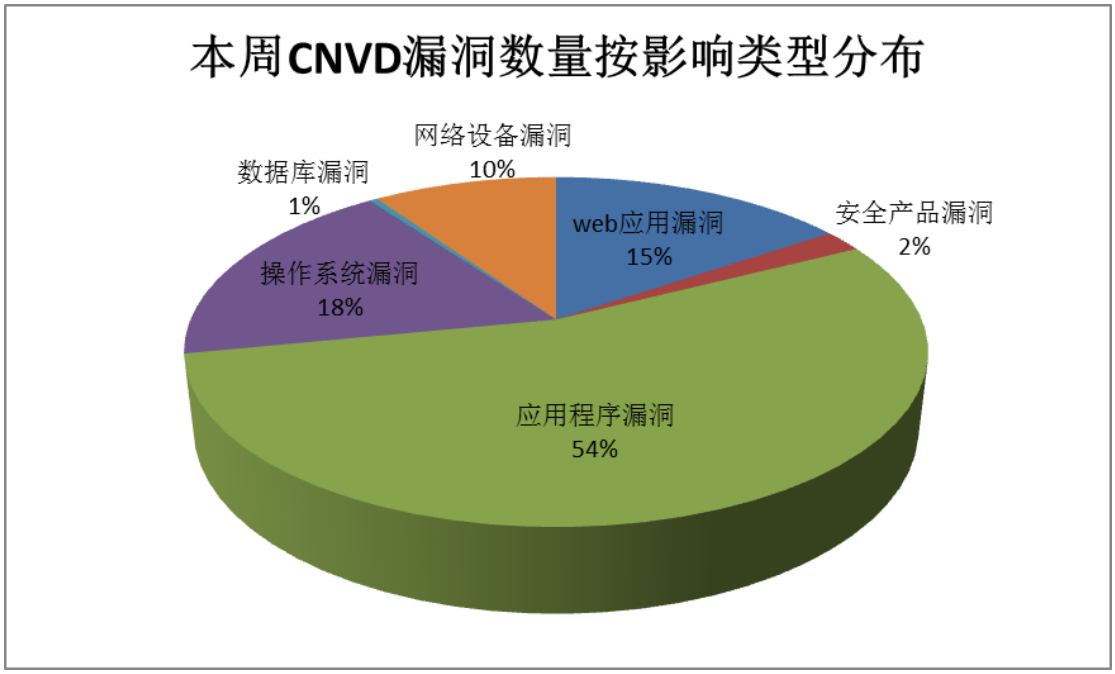

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Apple、Google 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	Adobe	53	11%
2	Apple	50	10%
3	Google	33	7%
4	Huawei	28	6%
5	ImageMagick	21	4%
6	IBM	17	3%
7	Cisco	15	3%
8	NetIQ	11	2%
9	Revive Adserver	9	2%
10	其他	254	52%

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 32 个电信行业漏洞，84 个移动互联网行业漏洞，9 个工控系统行业漏洞（如下图所示）。其中，“CoDeSys 堆栈缓冲区溢出漏洞、CoDeSys Web 服务器任意文件上传漏洞、多个 Cisco 产品本地权限提升漏洞、华为 Campus 系列交换机堆缓冲区溢出漏洞、多款华为 Quidway 交换机拒绝服务漏洞、华为交换机 Y.1731 拒绝服务漏洞、多个 Cisco 产品本地命令注入漏洞（CNVD-2017-04873）、Cambium Networks cnPilot R200/201 存在漏洞、CoDeSys 堆栈缓冲区溢出漏洞、CoDeSys Web 服务器任意文件上传漏洞”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/

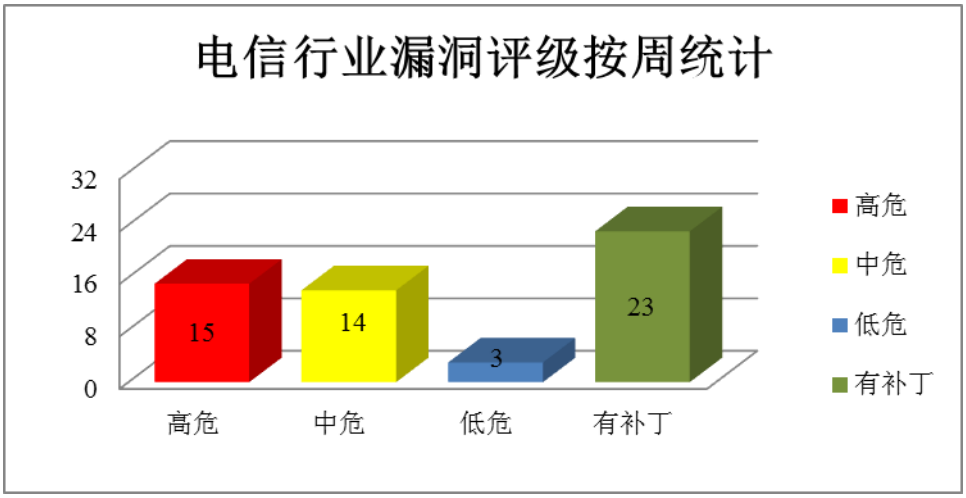

图 3 电信行业漏洞统计

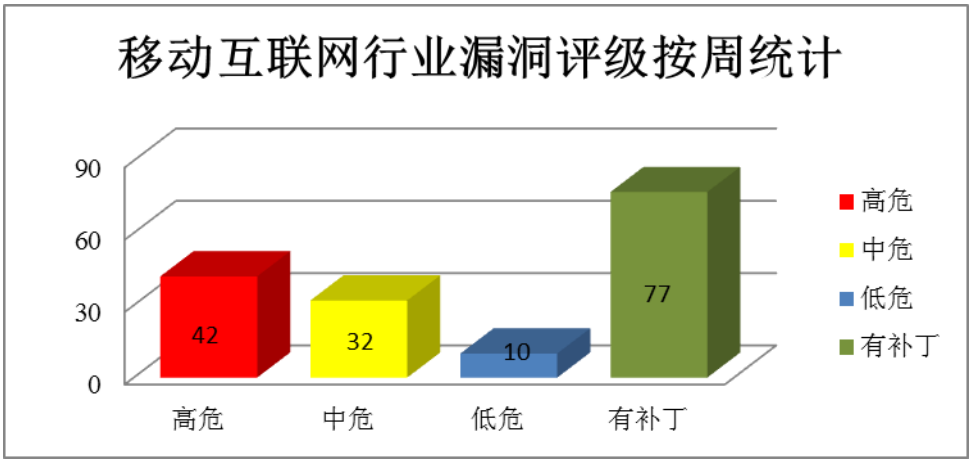

图 4 移动互联网行业漏洞统计

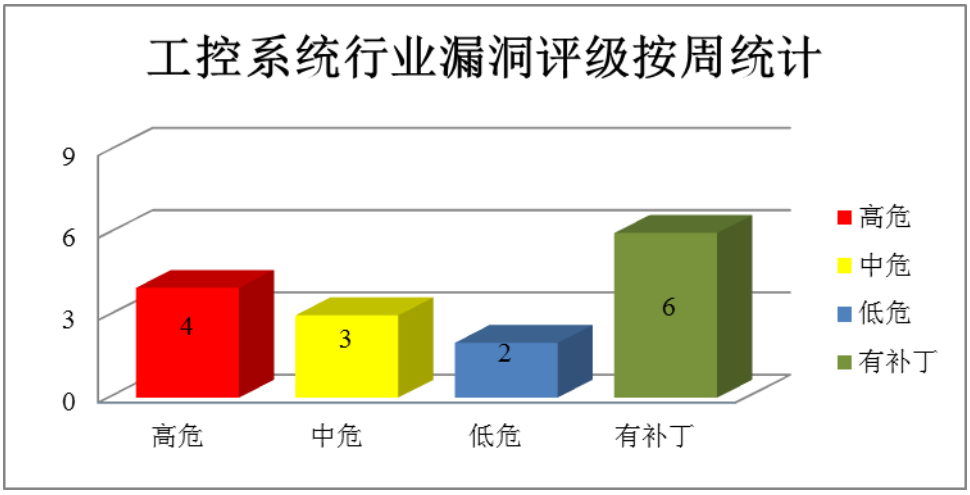

图 5 工控系统行业漏洞统计

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、Jackson 框架存在 Java 反序列化代码执行漏洞

Jackson 是一个开源的 java 序列化与反序列化工具。本周，该产品被披露存在 Java 反序列化代码执行漏洞，攻击者可利用漏洞在服务器主机上执行任意代码或系统指令，取得网站服务器的控制权。

CNVD 收录的相关漏洞包括：Jackson 框架 enableDefaultTyping 方法反序列化漏洞。该漏洞的综合评级为“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-2017-04483

2、Adobe 产品安全漏洞

Adobe Acrobat 和 Reader 是美国 Adobe 公司开发的一款可以用便携式文档格式出版所有的文档的编辑软件。本周，该产品被披露存在内存破坏漏洞，攻击者可利用漏洞控制受影响的系统，执行任意代码。

CNVD 收录的相关漏洞包括：Adobe Acrobat 和 Reader 内存破坏漏洞（CNVD-2017-04690、CNVD-2017-04691、CNVD-2017-04692、CNVD-2017-04693、CNVD-2017-04694、CNVD-2017-04695、CNVD-2017-04696、CNVD-2017-04697）。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-2017-04690

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04691

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04692

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04693

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04694

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04695

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04696

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04697

3、Google 产品安全漏洞

Google Android 是一款基于 Linux 开放性内核的手机操作系统。本周，该产品被披露存在权限提升漏洞，攻击者可利用漏洞提升权限。

CNVD 收录的相关漏洞包括：Google Android Broadcom Wi-Fi Driver 权限提升漏洞（CNVD-2017-04965、CNVD-2017-04966、CNVD-2017-04967、CNVD-2017-04968、CNVD-2017-04969、CNVD-2017-04576、CNVD-2017-04578、CNVD-2017-04579）。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-2017-04965

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04966

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04967

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04968

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04969

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04976

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04978

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04979

4、Huawei 产品安全漏洞

华为 Tecal RH1288 V2 等都是中国华为（Huawei）公司的服务器。华为 Campus S7700 等都是企业级园区交换机。华为 HiSuite 是一套用于 PC 端的手机助手软件。Huawei Vicky-AL00A/Victoria-AL00A 是一款智能手机。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞绕过安全限制、执行任意代码和发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：多款华为服务器缓冲区溢出漏洞、华为 Campus S7700/S9300/S9700 交换机安全绕过漏洞、华为 Campus 系列交换机堆缓冲区溢出漏洞、华为交换机 Y.1731 拒绝服务漏洞、华为 HiSuite 中间人攻击漏洞、华为手机 Bastet 组件存在多个缓冲区溢出漏洞（CNVD-2017-04679、CNVD-2017-04678）、华为手机 Bastet 组件存在多个缓冲区溢出漏洞。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-2017-04637

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04632

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05106

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05108

http://www.cnvd.org.cn/flaw/show/CNVD-2017-05109

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04679

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04678

http://www.cnvd.org.cn/flaw/show/CNVD-2017-04677

5、Linksys Smart Wi-Fi Routers 命令注入漏洞

Linksys Smart Wi-Fi Routers 是智能 Wi-Fi 路由器。本周，Linksys Smart Wi-Fi Routers 被披露存在命令注入漏洞，攻击者通过设备认证可以 root 权限在设备的操作系统上注入和执行恶意代码。目前，互联网上已经出现了针对该漏洞的攻击代码，厂商尚未发布漏洞修补程序。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-2017-05025

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-2017-04496	ImageMagick jng decoder 拒绝服务漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.imagemagick.org
CNVD-2017-04726	NetIQ Access Manager 远程代码执行漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://www.novell.com/support/kb/doc.php?id=7017807
CNVD-2017-04959	NetIQ Access Manager 访问认证凭据漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.netiq.com/support/kb/doc.php?id=7017818
CNVD-2017-04989	Erlang/OTP 堆缓冲区溢出漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/erlang/otp/pull/1108
CNVD-2017-05023	CoDeSys 堆栈缓冲区溢出漏洞	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：http://store.codesys.com/codesys-23.html
CNVD-2017-05030	多款 Brother 设备认证绕过漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：https://cxsecurity.com/blad/WLB-2017040064
CNVD-2017-05041	Cambium Networks cnPilot R200/201 存在漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：http://www.cambiumnetworks.com/

CNVD-2017-05084	Tenable Nessus Agent 模式本地权限提升漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：https://www.tenable.com/security/tns-2017-08
CNVD-2017-05090	GnuTLS 存在多个漏洞	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://www.gnutls.org/security.html
CNVD-2017-05113	DragonWave Horizon 硬编码凭据漏洞	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.dragonwaveinc.com/

表 4 部分重要高危漏洞列表

小结：本周，Jackson 被披露存在 Java 反序列化代码执行漏洞，攻击者可利用漏洞在服务器主机上执行任意代码或系统指令。此外，Adobe、Google、Huawei 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、绕过安全限制、提升权限或发起拒绝服务攻击等。另外，Linksys Smart Wi-Fi Routers 被披露存在命令注入漏洞，攻击者通过设备认证可以 root 权限在设备的操作系统上注入和执行恶意代码。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。

本周漏洞要闻速递

1. MySQL 曝中间人攻击 Riddle 漏洞

Riddle 是一个在 Oracle MySQL 5.5 和 5.6 客户端数据库中发现的高危安全漏洞。允许攻击者在中间人位置使用 Riddle 漏洞破坏 MySQL 客户端和服务器之间的 SSL 配置连接。此漏洞是一个非常危险的漏洞，因为首先它会影响 MySQL，其次会影响 SSL 连接。安全研究员 Pali Rohár 称，导致 Riddle 漏洞的原因是之前存在于 MySQL 数据库中的 BACKRONYM 漏洞没有被修复。Backronym 漏洞能在中间人攻击时用来泄露密码，即使流量经过加密。

参考链接：http://www.freebuf.com/news/132150.html

2. 数十款 Linksys 路由器曝高危漏洞，可致远程命令执行及敏感信息泄露

来自 IOACTIVE 的研究人员最近发现了存在于 Linksys 智能 Wifi 路由器中的漏洞。从低危到高危，其中六个可被攻击者远程利用。2 个漏洞能够让攻击者进行 DoS 攻击。通过发送一些请求或者滥用特定的 API，路由器会停止服务甚至重启。这样管理员就无法访问 web 管理界面了，而用户也无法链接网络，除非攻击者停止攻击。

参考链接：http://www.freebuf.com/news/132831.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