

国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2016 年 07 月 18 日-2016 年 07 月 24 日

2016 年第 30 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 370 个，其中高危漏洞 159 个、中危漏洞 178 个、低危漏洞 33 个。漏洞平均分为 6.53 分。本周收录的漏洞中，涉及 0day 漏洞 74 个（占 20%）。其中互联网上出现“TP-Link Wireless N Network Camera 操作系统命令注入漏洞、Apache Continuum 'saveInstallation.action'命令注入漏洞”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 648 个，与上周（419 个）环比增长 55%。

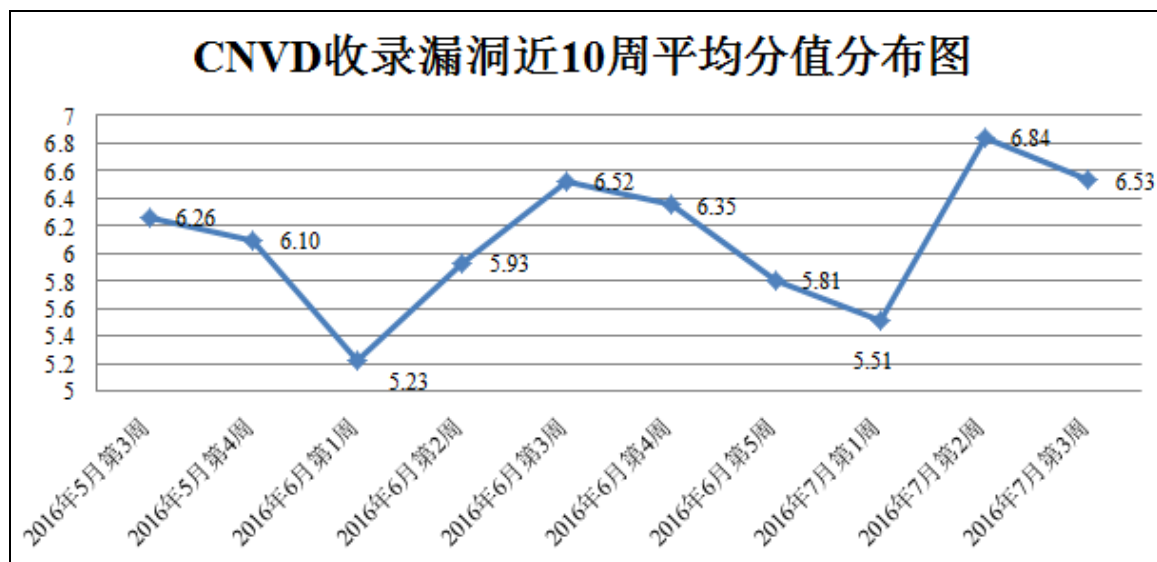


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 9 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 370 个漏洞。报送情况如表 1 所示。其中，奇虎(补天平台)、安天实验室、恒安嘉新、启

明星辰、等单位报送数量较多。补天平台、乌云、漏洞盒子、深圳市深信服电子科技有限公司、腾讯玄武实验室及其他个人白帽子向 CNVD 提交了 648 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)	406	406
安天实验室	352	0
恒安嘉新	258	15
启明星辰	209	5
天融信	58	0
杭州安恒信息技术有限公司	53	0
H3C	25	0
中国电信集团系统集成有限责任公司	23	0
绿盟科技	21	0
乌云	200	200
漏洞盒子	4	4
深圳市深信服电子科技有限公司	5	5
腾讯玄武实验室	1	1
CNCERT 四川分中心	1	1
个人	11	11
报送总计	1627	648
录入总计	370（去重）	648

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 370 个漏洞。其中应用程序漏洞 236 个，web 应用漏洞 66 个，网络设备漏洞 29 个，操作系统漏洞 23 个，数据库漏洞 8 个，安全产品漏洞 8 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	236
web 应用漏洞	66
网络设备漏洞	29
操作系统漏洞	23
数据库漏洞	8
安全产品漏洞	8

表 2 漏洞按影响类型统计表

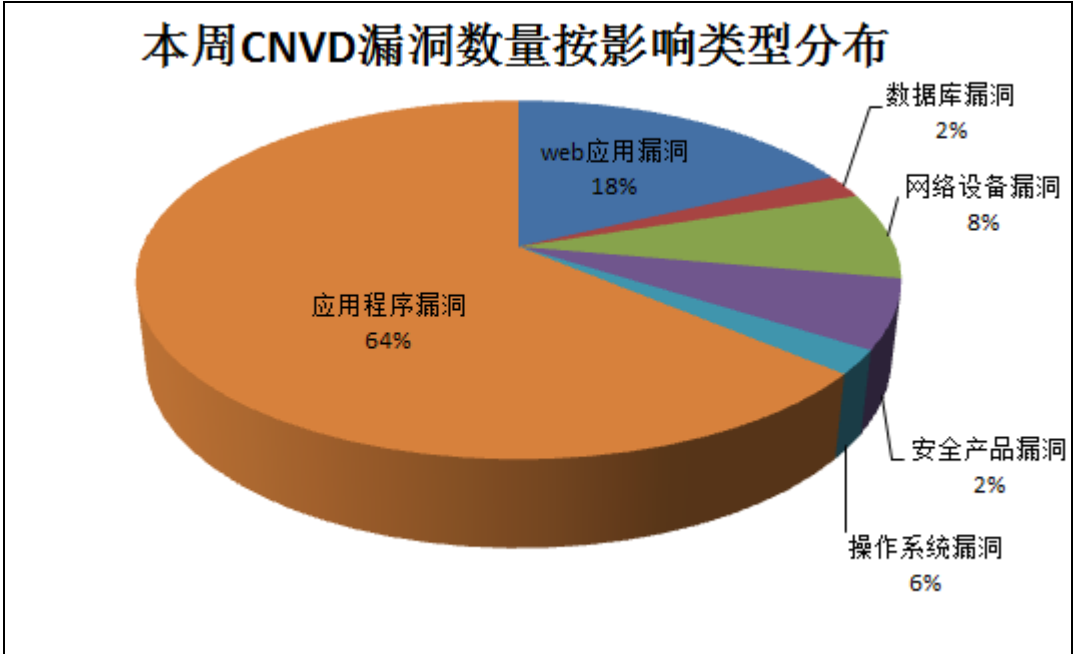


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Microsoft、Drupal 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	63	17%
2	Microsoft	24	6%
3	Drupal	18	5%
4	Oracle	14	4%
5	Huawei	11	3%
6	Cisco	11	3%
7	TYPO3	10	3%
8	WordPress	9	2%
9	OpenBSD	9	2%
10	其他	201	55%

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 个电信行业漏洞，4 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，“Oracle Database Server OJVM 存在未明漏洞、Oracle Database Server JDBC 存在未明漏洞、Oracle Database Server Portable Clusterware 存在未明漏洞、Oracle Database Server Data Pump Import 组件存在未明漏洞、Oracle Fusion Middleware GlassFish Server 组件存在未明漏洞、Oracle Fusion Middleware JDeveloper 组件存在未明漏洞漏洞、Huawei AR3200 Routers 远程代码执行漏洞、IBM Traveler XML 外部实体注入漏洞、Android 本地安全绕过漏洞、GE Proficy HMI SCADA CIMPPLICITY 本地提权漏洞等”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/>

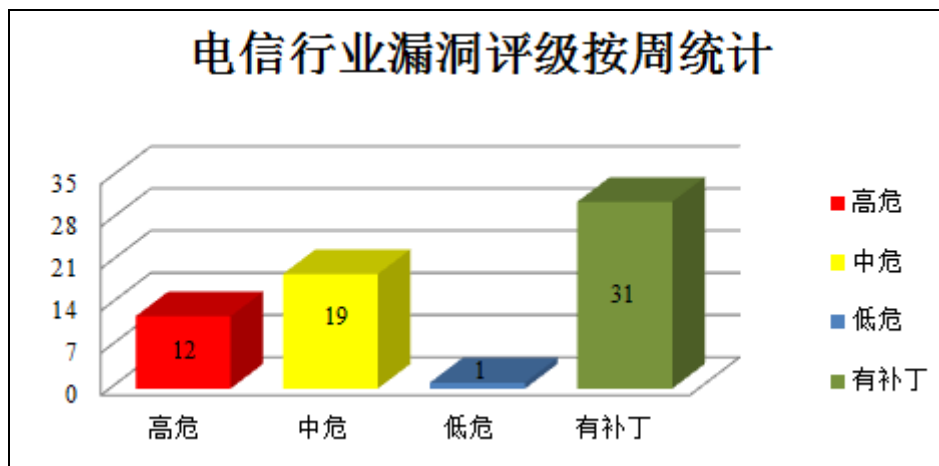


图 3 电信行业漏洞统计

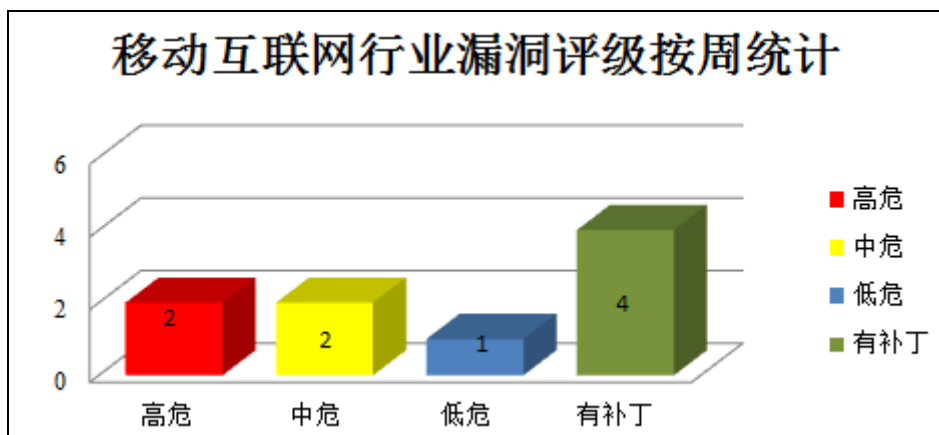


图 4 移动互联网行业漏洞统计

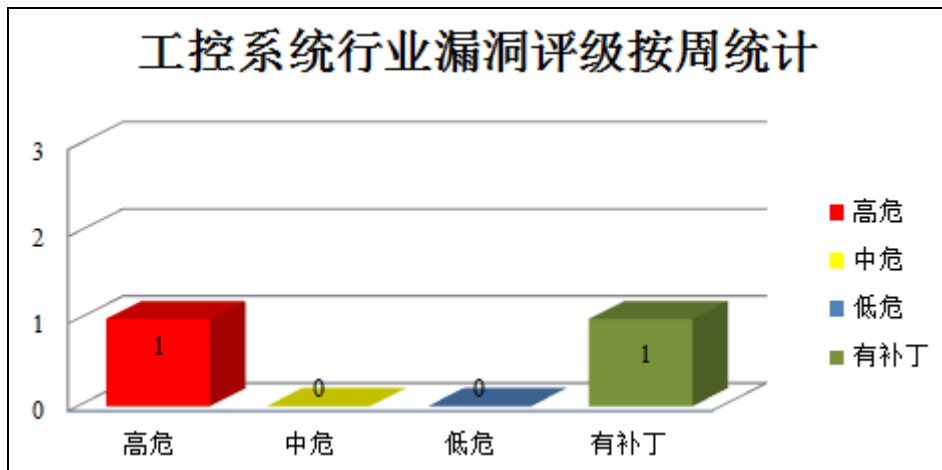


图 5 工控系统行业漏洞统计

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、Oracle 产品安全漏洞

7月19日，Oracle 发布了 2016 年 7 月份的安全更新，修复了其多款产品存在的 276 个安全漏洞。受影响的产品包括 Oracle 数据库（9 个）、中间件产品 Fusion Middleware（40 个）；企业管理器网格控制产品 Oracle Enterprise Manager Grid Control（10 个）、电子商务套装软件 Oracle E-Business Suite（23 个）、供应链套装软件 Oracle Supply Chain Products Suite（25 个）、Oracle Siebel 托管型 CRM 软件（16 个）；Hyperion（1 个）、PeopleSoft 产品（7 个）、JD Edwards 产品（1 个）、Primavera 产品（15 个）、Virtualization（4 个）、Retail Applications（16 个）、Communications Applications（16 个）、Health Sciences Applications（5 个）、Financial Services Applications（4 个）、Insurance Applications（8 个）、Utilities Applications（3 个）、Policy Automation（4 个）；Java SE（13 个）、Oracle Sun 系统产品（34 个）和 MySQL 数据库（22 个）。本次安全更新提供了针对 130 个高危漏洞的补丁，有 251 个漏洞可被远程利用。

CNVD 收录的相关漏洞包括：Oracle Database Server OJVM 存在未明漏洞、Oracle Database Server JDBC 存在未明漏洞、Oracle Database Server Portable Clusterware 存在未明漏洞、Oracle Database Server Data Pump Import 组件存在未明漏洞、Oracle Fusion Middleware GlassFish Server 组件存在未明漏洞、Oracle Fusion Middleware JDeveloper 组件存在未明漏洞、Oracle WebLogic Server 存在未明漏洞（CNVD-2016-05196、CNVD-2016-05195）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/3895>

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。该产品支持跨屏幕和浏览器查看应用程序、内容和视频。本周, 上述产品被披露存在内存破坏漏洞, 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 内存破坏漏洞 (CNVD-2016-04877、CNVD-2016-04878、CNVD-2016-04872、CNVD-2016-04882、CNVD-2016-04883、CNVD-2016-04874、CNVD-2016-04875、CNVD-2016-04876) 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-2016-04877>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04878>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04872>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04882>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04883>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04874>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04875>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04876>

3、Huawei 产品安全漏洞

Huawei Honor 4C (华为荣耀 4C) 是中国华为 (Huawei) 公司的一款智能手机产品。Huawei P8 是中国华为 (Huawei) 公司的一款智能手机产品。Huawei Honor6 是一款智能手机产品。本周, 上述产品被披露存在输入验证、本地提权和缓冲区溢出漏洞, 攻击者可利用漏洞提升权限和执行任意代码。

CNVD 收录的相关漏洞包括: Huawei Honor 4C 驱动输入验证漏洞、Huawei Honor6 Smart Phone 本地提权漏洞、Huawei P8 本地缓冲区溢出漏洞、Huawei Honor 4C 驱动输入验证漏洞 (CNVD-2016-05174、CNVD-2016-05175、CNVD-2016-05176、CNVD-2016-05177)、Huawei P8 本地缓冲区溢出漏洞 (CNVD-2016-04990) 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-2016-05173>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05049>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04991>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05174>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05175>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05176>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-00177>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-04990>

4、OpenBSD 产品安全漏洞

OpenBSD 是加拿大 OpenBSD 项目组开发的一套跨平台的、基于 BSD 的类 UNIX 操作系统。本周，上述产品被披露存在内存破坏和拒绝服务漏洞，攻击者可利用漏洞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：OpenBSD 存在多个漏洞（CNVD-2016-05204、CNVD-2016-05203、CNVD-2016-05202、CNVD-2016-05201、CNVD-2016-05200、CNVD-2016-05199、CNVD-2016-05206、CNVD-2016-05205）等。上述漏洞的综合评级为“高危”。目前，厂商尚未发布上述漏洞的修补程序。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-2016-05204>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05203>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05202>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05201>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05200>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05199>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05206>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-05205>

5、D-Link DCS-930L Camera 命令注入漏洞

D-Link DCS-930L 是友讯（D-Link）公司的一款无线监控摄像头。本周，D-Link DCS-930L 被披露存在命令注入漏洞。攻击者可利用漏洞执行任意命令。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-2016-05244>

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-2016-04860	Drupal Coder 远程代码执行漏洞	高	厂商已发布修复方案，请及时下载更新： https://www.drupal.org/project/coder
CNVD-2016-04859	Drupal Webform Multiple File Upload 远程代码执行漏洞	高	厂商已发布修复方案，请及时下载更新： https://www.drupal.org/project/webform_multifile
CNVD-2016-04861	Drupal RESTWS 远程代码执行漏洞	高	厂商已发布修复方案，请及时下载更新： https://www.drupal.org/project/restw

			s
CNVD-2016-04906	Linux util-linux 本地提权漏洞	高	暂无
CNVD-2016-04922	Microsoft Windows Server 权限提升漏洞 (CNVD-2016-04922)	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://technet.microsoft.com/security/bulletin/MS16-090
CNVD-2016-04929	Microsoft Edge 脚本引擎内存破坏漏洞	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://technet.microsoft.com/security/bulletin/MS16-085
CNVD-2016-04934	Schneider Electric Pelco Digital Sentry Video Management System 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，补丁获取链接： http://www.schneider-electric.com/www/en/download/document/SEVD-2016-153-01
CNVD-2016-04933	多款 Moxa 产品身份验证绕过漏洞	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.moxa.com/support/sarch_result.aspx?type=soft&prod_id=73&type_id=4
CNVD-2016-04930	TeamPass 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://teampass.net/
CNVD-2016-04931	JetBrains PyCharm Professional 本地代码执行漏洞	高	暂无

表 4 部分重要高危漏洞列表

小结：7 月 19 日，Oracle 发布了 2016 年 7 月份的安全更新，修复了其多款产品存在的 276 个安全漏洞。其中，本次安全更新提供了针对 130 个高危漏洞的补丁，有 251 个漏洞可被远程利用。此外，Adobe、Huawei、OpenBSD 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞执行任意代码、提升权限和发起拒绝服务攻击等。另外，D-Link DCS-930L 被披露存在一个“高危”漏洞。攻击者可利用漏洞执行任意命令。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. Ubuntu 官网论坛遭入侵

近日 Ubuntu 官方论坛被黑，泄露了超过 200 万数据，本次泄露的用户数据包括 IP 地址、用户名和电子邮件地址。经过深入调查后，发现罪魁祸首是论坛插件 Forumrunner 的 SQL 注入 Xday，因为没有及时打上补丁，才导致了用户数据的泄露。攻击者利用

SQL 注入漏洞，从论坛数据库里下载了部分数据，即约 200 万用户的用户名、电子邮件地址和 IP 地址信息。

参考链接：<http://www.freebuf.com/news/109312.html>

2. D-Link 云摄像头超过 120 款产品存在漏洞，约 40 万台设备受影响

之前也有过摄像头存在安全漏洞，隐私被泄露出去的事件。这次事件的主角轮到了 D-Link 云摄像头。一位叫 Stephen Ridley 的安全研究员发现了 D-Link 云摄像头漏洞的存在，并且他还发现了超过 120 款产品存在相同的漏洞。自从 RCE 漏洞可以通过网络连接被执行以后，任何存在这一漏洞 D-Link 设备通过一个 ping 命令就能成功连接上，这存在潜在的危险。研究员声称总共超过 40 万的 D-link 设备目前可以在线使用。

参考链接：<http://www.freebuf.com/news/108870.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