

信息安全漏洞周报

2016 年 03 月 14 日-2016 年 03 月 20 日

2016 年第 12 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**高**。

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 143 个，其中高危漏洞 71 个、中危漏洞 69 个、低危漏洞 3 个。漏洞平均分为 7.03 分。本周收录的漏洞中，涉及 0day 漏洞 15 个（占 10%）。本周，互联网上披露了 Apache Struts2 存在的一处远程代码执行漏洞，目前暂未存在有效的远程利用代码，但已经有验证信息，不排除后续出现大规模攻击的可能，CNVD 提醒用户及时下载补丁更新。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 906 个，与上周（1214 个）环比下降 25%。

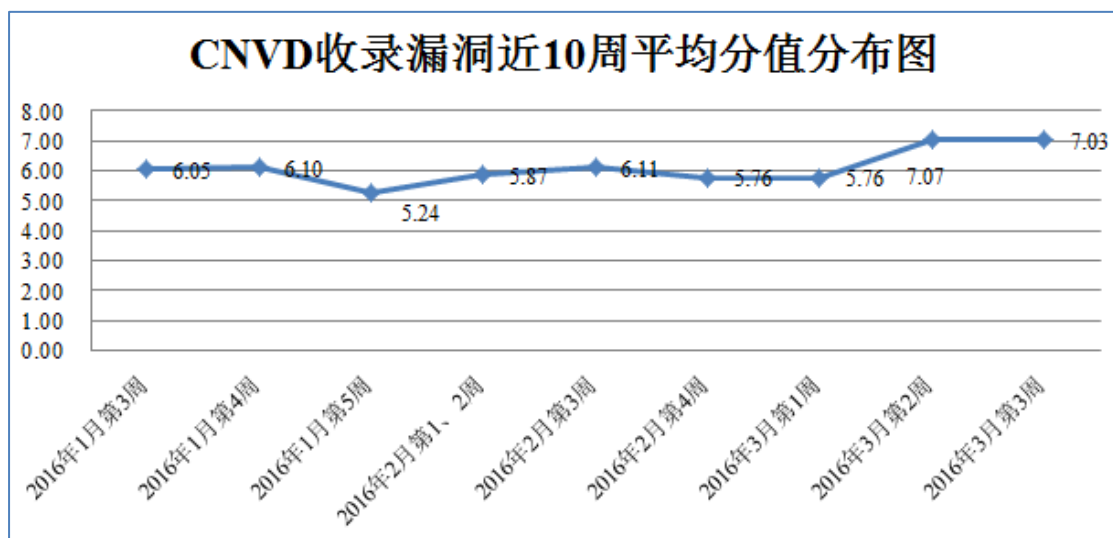


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 7 家成员单位、合作伙伴及个人报送了本周收录的全部 143 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、天融信、绿盟科技等单位报送

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、High-Tech Bridge Security Research Lab、山东安云信息技术有限公司、河北翎贺计算机信息技术有限公司及白帽子向 CNVD 提交了 906 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)	340	340
安天实验室	125	0
天融信	114	0
绿盟科技	80	0
启明星辰	76	0
恒安嘉新	46	0
H3C	2	0
乌云	469	469
漏洞盒子	56	56
High-Tech Bridge Security Research Lab	3	3
深圳市深信服电子科技有限公司	1	1
山东安云信息技术有限公司	1	1
河北翎贺计算机信息技术有限公司	1	1
CNCERT 宁夏分中心	1	1
CNCERT 福建分中心	1	1
个人	33	33
报送总计	1349	906
录入总计	143（去重）	906

表 1 成员单位上报漏洞统计表



本周漏洞按类型和厂商统计

本周，CNVD 收录了 143 个漏洞。其中应用程序漏洞 107 个，网络设备漏洞 17 个，操作系统漏洞 15 个，Web 应用漏洞 2 个，安全产品漏洞 2 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	107
网络设备漏洞	17
操作系统漏洞	15
Web 应用漏洞	2
安全产品漏洞	2

表 2 漏洞按影响类型统计表

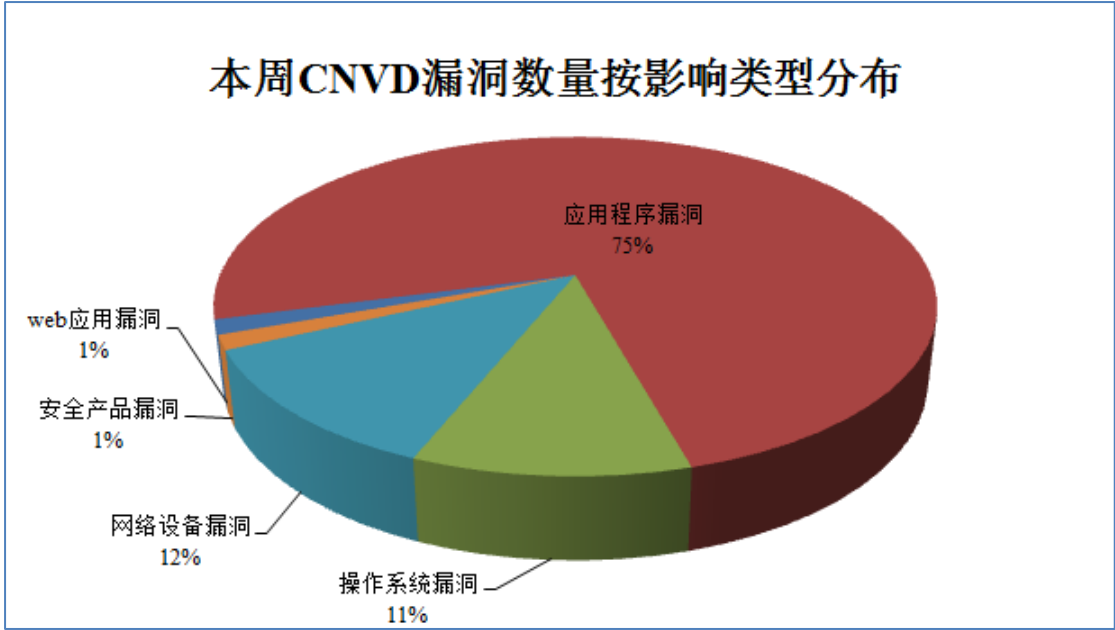


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Mozilla、Adobe、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	Mozilla	42	29%
2	Adobe	24	17%
3	Google	16	11%
4	Cisco	7	5%
5	IBM	7	5%
6	Schneider Electric	6	4%
7	Apache	6	4%
8	OpenJPEG	3	2%
9	Netgear	3	2%

10	其他	29	21%
----	----	----	-----

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 7 个电信行业漏洞、13 个移动互联网漏洞、5 个工控系统行业漏洞（如下图所示）。其中，“Android MediaTek Wi-Fi 内核驱动程序权限获取漏洞、Android MediaTek connectivity 权限获取漏洞、Android mediaserver 权限获取漏洞”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/>

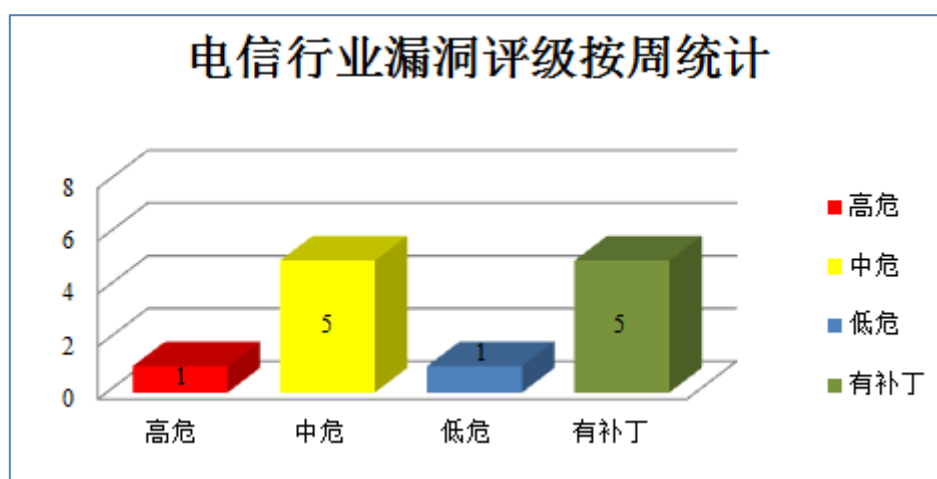


图 3 电信行业漏洞统计

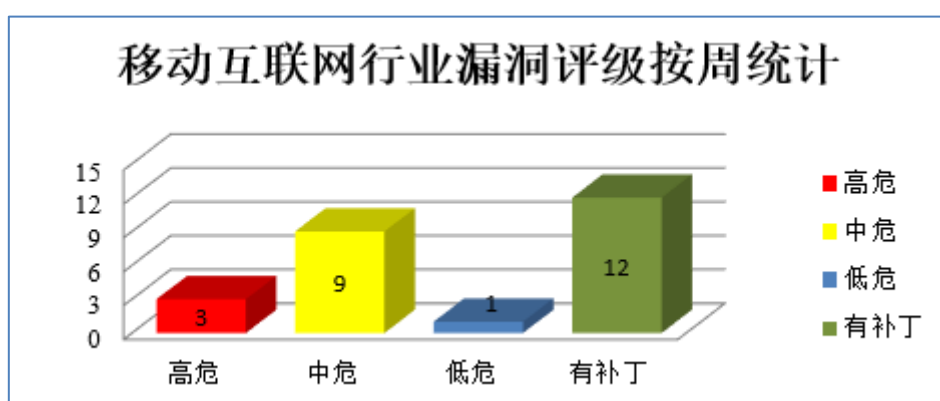


图 4 移动互联网行业漏洞统计

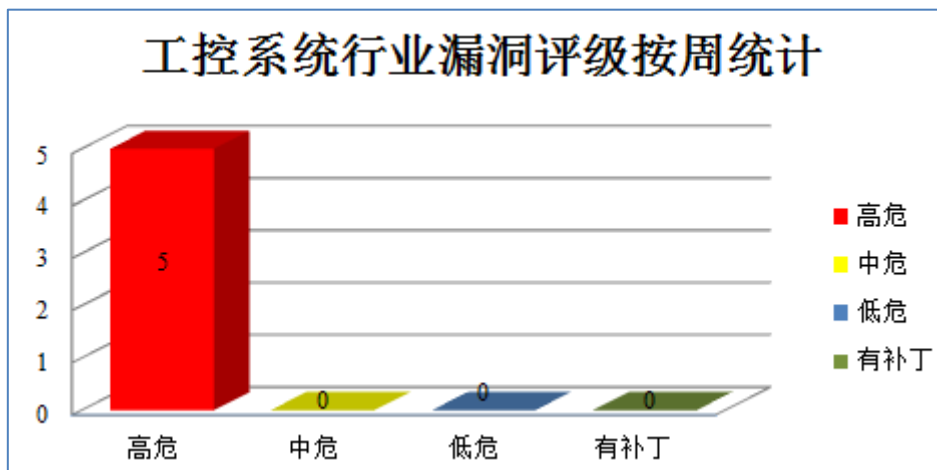


图 5 工控系统行业漏洞统计

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、Apache 产品安全漏洞

Apache Struts 是美国阿帕奇（Apache）软件基金会负责维护的一款用于创建企业级 Java Web 应用的开源框架。Jetspeed 是美国阿帕奇（Apache）软件基金会的一套使用 Java 和 XML 开发的开放门户平台和企业信息门户网站。Apache ActiveMQ 是流行的消息传输和集成模式提供程序。本周，上述产品被披露存在跨站脚本和远程代码执行漏洞，远程攻击者可利用漏洞进行跨站脚本攻击和执行任意代码。

CNVD 收录的相关漏洞包括：Apache Struts2 远程代码执行漏洞、Apache Struts 1 18NInterceptor 跨站脚本漏洞、Apache Jetspeed 跨站脚本漏洞（CNVD-2016-01717）、Apache Jetspeed 跨站脚本漏洞、Apache ActiveMQ Web Console 跨站脚本漏洞、Apache ActiveMQ Web Console 单击劫持漏洞。其中，“Apache Struts2 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-2016-01714>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01715>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01717>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01716>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01695>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01694>

2、Mozilla 产品安全漏洞

Firefox 是一款开源 Web 浏览器；Firefox ESR 是 Firefox 的一个延长支持版本。Gr

aphite 是一套使用 Python 语言编写、采用 Django 框架的企业级开源系统监控工具。本周，上述产品被披露存在代码执行漏洞，远程攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Mozilla Firefox 和 Firefox ESR Graphite 2 代码执行漏洞（CNVD-2016-01597、CNVD-2016-01596、CNVD-2016-01595、CNVD-2016-01594、CNVD-2016-01593、CNVD-2016-01592、CNVD-2016-01591、CNVD-2016-01682）。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-2016-01597>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01596>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01595>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01594>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01593>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01592>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01591>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01682>

3、Google 产品安全漏洞

Android 是美国谷歌（Google）公司和开放手持设备联盟（简称 OHA）共同开发的一套以 Linux 为基础的开源操作系统。本周，上述产品被披露存在信息泄露、安全绕过和权限获取漏洞，远程攻击者可利用漏洞获取敏感信息、绕过安全限制和获取权限。

CNVD 收录的相关漏洞包括：Android Linux kernel 安全绕过漏洞、Android MediaTek Wi-Fi 内核驱动程序权限获取漏洞、Android MediaTek connectivity 权限获取漏洞、Android Linux kernel 信息泄露漏洞、Android libstagefright 安全绕过漏洞、Android Wi device Trusted Application 信息泄露漏洞、Android mediaserver 权限获取漏洞、Android mediaserver 安全绕过漏洞。其中“Android MediaTek Wi-Fi 内核驱动程序权限获取漏洞、Android MediaTek connectivity 权限获取漏洞、Android mediaserver 权限获取漏洞”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-2016-01703>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01704>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01667>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01668>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01669>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01670>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01671>
<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01674>

4、Adobe 产品安全漏洞

Adobe Flash Player 是一款多媒体播放器产品; Adobe AIR SDK 和 Adobe AIR SDK & Compiler 都是适用于 Adobe AIR 的标准开发工具包。本周, 该产品被披露存在内存错误引用漏洞, 攻击者利用漏洞可执行任意代码。

CNVD 收录的相关漏洞包括: Adobe Flash Player 内存错误引用漏洞 (CNVD-2016-01613、CNVD-2016-01614、CNVD-2016-01615、CNVD-2016-01621、CNVD-2016-01623、CNVD-2016-01627、CNVD-2016-01628、CNVD-2016-01629)。上述漏洞的综合评级均为“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-2016-01613>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01614>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01615>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01621>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01623>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01627>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01628>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-01629>

5、D-Link 缓冲区溢出漏洞

D-Link 是网络设备和解决方案提供商, 产品包括多种路由器设备。本周, 多个 D-Link 产品被披露存在缓冲区溢出漏洞, 攻击者可利用漏洞执行任意代码。目前, 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-2016-01688>

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-2016-01599	Microsoft Internet Explorer 内存破坏漏洞 (CNVD-2016-01599)	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/MS15-106
CNVD-2016-01600	Cisco DPC2203 和 EPC2203 设备缓冲区溢出漏洞	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: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-cmre
CNVD-2016-01601	Cisco DPQ3925 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: https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-cmre

			r/content/CiscoSecurityAdvisory/cisco-sa-20160309-cmdos
CNVD-2016-01602	Cisco DPC3939B 和 DPC3941 信息泄露漏洞	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： https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-rgid
CNVD-2016-01605	Microsoft Office 内存破坏漏洞（CNVD-2016-01605）	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/MS16-029
CNVD-2016-01598	Cisco ASA 5500 Content Security and Control Security Services Module 拒绝服务漏洞	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： https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160309-csc
CNVD-2016-01636	Google Chrome Blink 代码执行漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://googlechromereleases.blogspot.com/2016/03/stable-channel-update_8.html
CNVD-2016-01635	Google Chrome Blink 代码执行漏洞（CNVD-2016-01635）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://googlechromereleases.blogspot.com/2016/03/stable-channel-update_8.html
CNVD-2016-01638	Google Chrome 远程代码执行漏洞（CNVD-2016-01638）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://googlechromereleases.blogspot.com/2016/03/stable-channel-update_8.html
CNVD-2016-01664	Samba 内部 DNS 服务器越界读漏洞	高	Samba 已经为此发布了一个安全公告（CVE-2016-0771）以及相应补丁： https://www.samba.org/samba/security/CVE-2016-0771.html

表 4 部分重要高危漏洞列表

小结：本周，Apache 产品被披露存在跨站脚本和远程代码执行漏洞，远程攻击者可利用漏洞进行跨站脚本攻击和执行任意代码。此外，Mozilla、Google、Adobe 等多款产品被披露存在多个安全漏洞，攻击者利用漏洞可获得敏感信息、绕过安全限制、进行跨站脚本攻击和执行任意代码等。除 D-Link 外，Cisco 的多款网络设备也被披露存在多

个漏洞。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. Stagefright 漏洞 exp 公布，数百万安卓手机仍受影响

Stagefright 是安卓设备中的一个软件库，用于解析视频和其他的媒体文件。去年 7 月份，安卓系统的 Stagefright 库被爆出一个重大的安全问题，攻击者可以利用一条精心制作的信息或者 web 页面在受害者设备上执行恶意代码。全球有数亿的安卓用户受到该漏洞的影响。现如今以色列的安全团队称，他们已经写出了 Stagefright 漏洞的 exp。目前仍然有数百万未更新补丁的安卓设备，他们的 exp 会绕过安卓的安全屏障继续感染这些设备。

参考链接：<http://www.freebuf.com/news/99306.html>

2. 反 DDoS 安全公司 Staminus 遭网络攻击，敏感数据泄露

一伙不明身份的黑客攻击了 DDoS 攻击防护公司 Staminus，并从其服务器上窃取了敏感信息。Staminus 是一家美国公司，目前主要致力于 DDoS 攻击防护研究。目前在已公布的 Hastebin 链接中，攻击者称他们能够窃取 Staminus 公司的数据库，Intrepid 服务数据库等。该公司尚未对该事件做出说明，但该公司已经开始恢复网络服务。

参考链接：<http://www.freebuf.com/news/98642.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