国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2018 年 2 月 12 日-2018 年 2 月 25 日 **2018 年第7、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 146 个，其中高危漏洞 31 个、中危漏洞 95 个、低危漏洞 20 个。漏洞平均分值为 5.56。本周收录的漏洞中，涉及 0day 漏洞 102 个（占 36%），其中互联网上出现“Joomla! Component CW Tags SQL 注入漏洞、RISE Ultimate Project Manager SQL 注入漏洞”等零日代码攻击漏洞。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 374 个，与上周（495）个环比降低 24%。

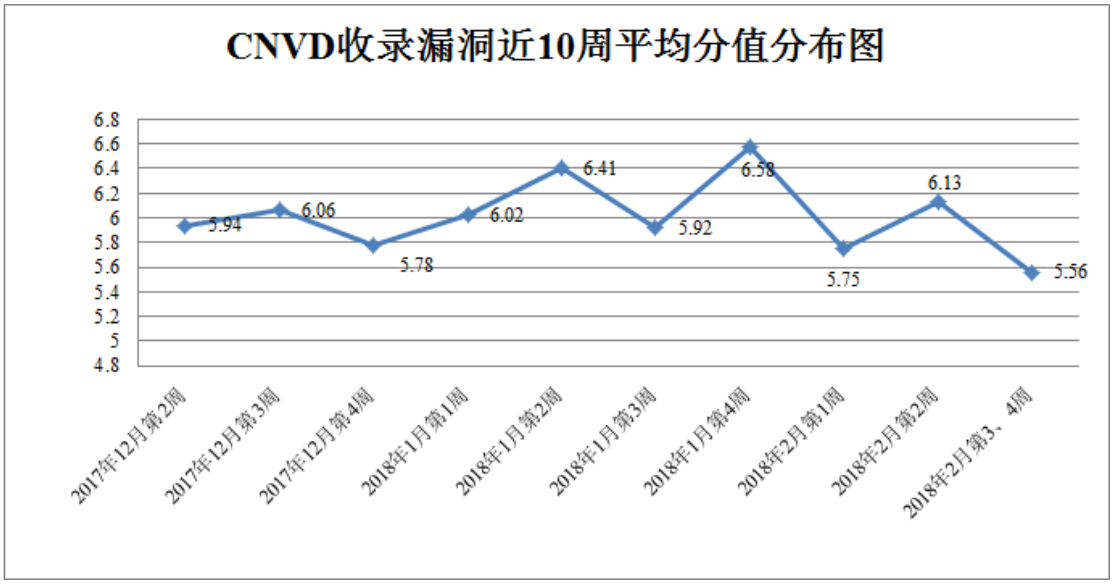

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，蓝盾信息安全技术有限公司、华为技术有限公司、北京数字观星科技有限公司等单位报送公开收集的漏洞数量较多。福建省海峡信息技术有限公司、四川虹微技术有限公司（子午攻防实验室）、南京联成科技发展股份有限公

司、中新网络信息安全股份有限公司、常州瑞新网络科技股份有限公司及其他个人白帽子向 CNVD 提交了 374 个以事件型漏洞为主的原创漏洞，其中包括 360 网神（补天平台）和漏洞盒子向 CNVD 共享的白帽子报送的 195 条原创漏洞信息。

表 1 漏洞报送情况统计表

报送单位或个人	漏洞报送数量	原创漏洞数量
蓝盾信息安全技术有限公司	299	0
华为技术有限公司	168	0
漏洞盒子	113	113
360 网神（补天平台）	82	82
北京数字观星科技有限公司	41	0
知道创宇	1	0
福建省海峡信息技术有限公司	21	21
四川虹微技术有限公司（子午攻防实验室）	5	5
南京联成科技发展股份有限公司	4	4
中新网络信息安全股份有限公司	1	1
常州瑞新网络科技股份有限公司	1	1
CNCERT 山西分中心	26	26
CNCERT 吉林分中心	5	5
CNCERT 新疆分中心	5	5
CNCERT 福建分中心	4	4
CNCERT 甘肃分中心	2	2
CNCERT 湖南分中心	2	2
CNCERT 上海分中心	2	2
CNCERT 贵州分中心	1	1

CNCERT 安徽分中心	1	1
个人	99	99
报送总计	883	374

本周漏洞按类型和厂商统计

本周，CNVD 收录了 146 个漏洞。其中应用程序漏洞 71 个，安全产品漏洞 28 个，操作系统漏洞 22 个，WEB 应用漏洞 19 个，网络设备漏洞 6 个。

表 2 漏洞按影响类型统计表

漏洞影响对象类型	漏洞数量
应用程序漏洞	71
安全产品漏洞	28
操作系统漏洞	22
WEB 应用漏洞	19
网络设备漏洞	6

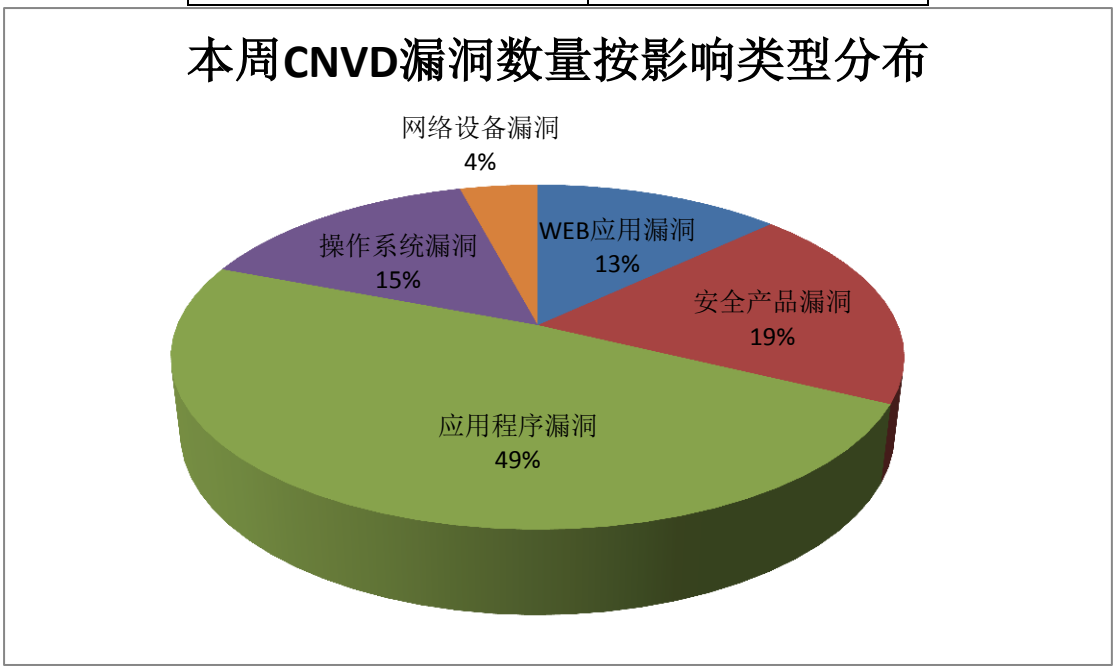

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Jiangmin、Extreme Networks、NetGain Systems 等多家厂商的产品，部分漏洞数量按厂商统计如表 3 所示。

表 3 漏洞产品涉及厂商分布统计表

序号	厂商（产品）	漏洞数量	所占比例
1	Jiangmin	21	14%
2	Extreme Networks	11	8%

3	Apache	9	6%
4	NetGain Systems	8	5%
5	IBM	7	5%
6	ClamAV	7	5%
7	Red Hat	7	5%
8	CloudBees	6	4%
9	Linux	6	4%
10	其他	64	44%

本周行业漏洞收录情况

本周，CNVD 收录了 4 个电信行业漏洞，2 个移动互联网行业漏洞，1 个工控行业漏洞（如下图所示）。其中，“多款 Huawei 产品 eSap software platform 堆缓冲区溢出漏洞、Apple iOS/watchOS/tvOS/macOS High Sierra 内存破坏漏洞”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/

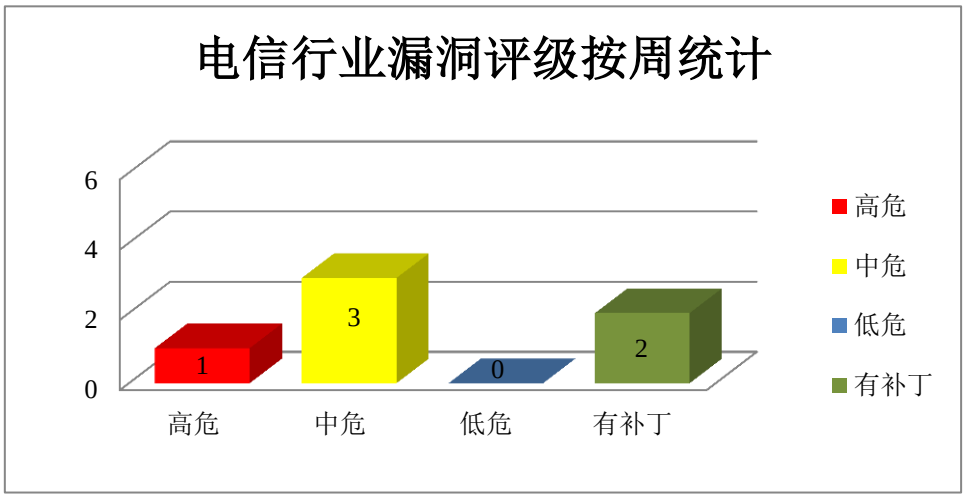

图 3 电信行业漏洞统计

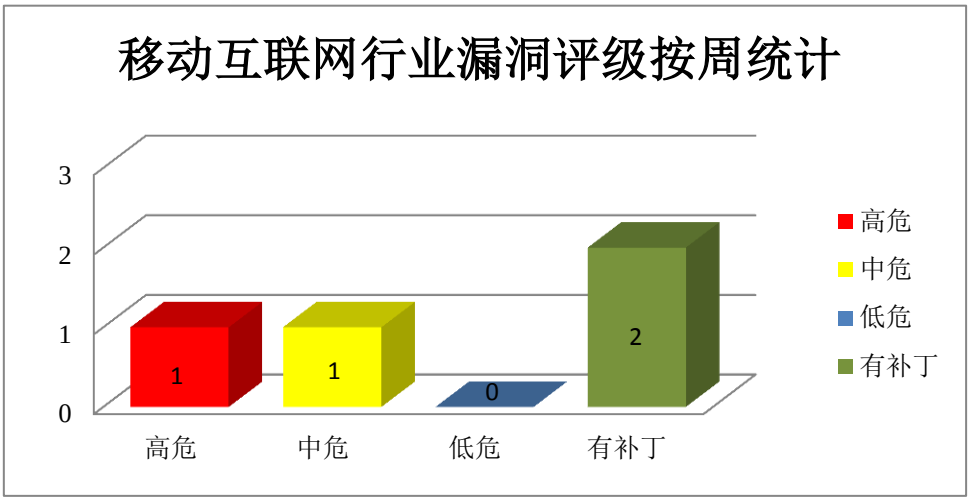

图 4 移动互联网行业漏洞统计

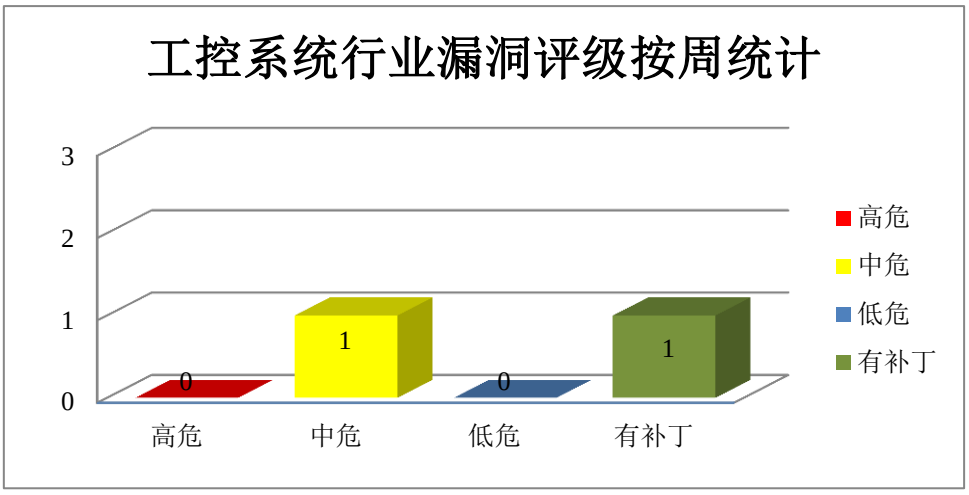

图 5 工控行业漏洞统计

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、Jiangmin 产品安全漏洞

Jiangmin Antivirus 是中国江民（Jiangmin）新科技术公司的一套在线杀毒软件。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：Jiangmin Antivirus 拒绝服务漏洞（CNVD-2018-03290、CNVD-2018-03291、CNVD-2018-03292、CNVD-2018-03293、CNVD-2018-03294、CNVD-2018-03295、CNVD-2018-03296、CNVD-2018-03297）。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-2018-03290

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03291

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03292

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03293

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03294

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03295

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03296

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03297

2、Apache 产品安全漏洞

Apache POI 是美国阿帕奇（Apache）软件基金会的一个开源函数库。 Apache Jmeter 是一款开源的 Java 应用程序；Apache Hadoop 是一套开源的分布式系统基础架构；Apache NiFi 是一套基于数据流的数据处理和分发系统；Apache Guacamole 是一款无客户端远程桌面网关。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞获取敏感信息、执行任意代码或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Apache Geode cluster 信息泄露漏洞、Apache Geode 代码执行漏洞、Apache Guacamole terminal emulator 缓冲区溢出漏洞、Apache Hadoop YARN NodeManager 密码泄露漏洞、Apache Hadoop 信息泄露漏洞（CNVD-2018-03273）、Apache NiFi 代码执行漏洞、Apache POI 拒绝服务漏洞（CNVD-2018-03242）、Apache JMeter 远程命令执行漏洞。其中，“Apache POI 拒绝服务漏洞（CNVD-2018-03242）、Apache JMeter 远程命令执行漏洞”的综合评级为“高危”。目前，厂商已经发布了除“Apache JMeter 远程命令执行漏洞”以外漏洞的修补程序。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-2018-03221

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03254

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03281

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03249

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03273

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03217

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03242

http://www.cnvd.org.cn/flaw/show/CNVD-2018-03472

3、Extreme Networks 产品安全漏洞

Extreme Networks ExtremeWireless WiNG 是美国极进网络（Extreme Networks）公司的一款无线接入解决方案。本周，该产品被披露存在多个漏洞，攻击者可利用漏洞发起拒绝服务攻击、提升权限或执行任意代码等。

CNVD 收录的相关漏洞包括：Extreme Networks ExtremeWireless WiNG 堆溢出漏洞（CNVD-2018-03320、CNVD-2018-03321）、Extreme Networks ExtremeWireless WiNG 拒绝服务漏洞（CNVD-2018-03323、CNVD-2018-03324）、Extreme Networks ExtremeWireless WiNG 权限提升漏洞、Extreme Networks ExtremeWireless WiNG 身份验证

绕过漏洞、Extreme Networks ExtremeWireless WiNG 硬编码 AES 密钥漏洞、Extreme Networks ExtremeWireless WiNG 栈溢出漏洞（CNVD-2018-03317）。其中，“Extreme Networks ExtremeWireless WiNG 拒绝服务漏洞（CNVD-2018-03323、CNVD-2018-03324）、Extreme Networks ExtremeWireless WiNG 权限提升漏洞”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-2018-03320
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03321
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03323
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03324
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03326
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03318
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03325
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03317

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的开源操作系统 Linux 所使用的内核。本周，该产品被披露存在拒绝服务、信息泄露和内存错误引用漏洞漏洞，攻击者可利用漏洞发起拒绝服务攻击或泄露敏感信息等。

CNVD 收录的相关漏洞包括：Linux kernel 拒绝服务漏洞（CNVD-2018-03215、CNVD-2018-03255、CNVD-2018-03256）、Linux kernel 内存错误引用漏洞（CNVD-2018-03259、CNVD-2018-03260）、Linux kernel 信息泄露漏洞（CNVD-2018-03263）。其中，“Linux kernel 内存错误引用漏洞（CNVD-2018-03259）”的综合评级为“高危”。目前，厂商已经发布了除“Linux kernel 拒绝服务漏洞（CNVD-2018-03255）”以外漏洞的修补程序。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-2018-03215
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03255
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03256
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03259
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03260
http://www.cnvd.org.cn/flaw/show/CNVD-2018-03263

5、 Joomla! Component CW Tags SQL 注入漏洞

Joomla!是美国 Open Source Matters 团队开发的一套开源的内容管理系统(CMS)。本周，Joomla!被披露存在 SQL 注入漏洞，攻击者可利用该漏洞危及应用程序，访问或修改数据，或利用底层数据库中潜在的漏洞。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.c

n/flaw/show/CNVD-2018-03430

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

表 4 部分重要高危漏洞列表

CNVD 编号	漏洞名称	综合评级	修复方式
CNVD-2018-03218	GitHub Electron 任意命令执行漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://github.com/electron/electron/releases/tag/v1.8.2-beta.4
CNVD-2018-03232	ClamAV 内存错误引用漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://blog.clamav.net/2018/01/clamav-0993-has-been-released.html
CNVD-2018-03233	ClamAV 缓冲区越边界读取漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://blog.clamav.net/2018/01/clamav-0993-has-been-released.html
CNVD-2018-03239	ClamAV 空指针解引用漏洞	高	厂商已发布漏洞修复程序，请及时关注更新：http://blog.clamav.net/2018/01/clamav-0993-has-been-released.html
CNVD-2018-03258	MC RSA Authentication Manager Security Console SQL 注入漏洞	高	目前厂商已发布升级补丁以修复漏洞，详情请关注厂商主页：http://www.emc2.com
CNVD-2018-03259	Linux kernel 内存错误引用漏洞（CNVD-2018-03259）	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.13.6
CNVD-2018-03276	NetIQ Access Manager 任意代码执行漏洞	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=7022443
CNVD-2018-03424	Apple macOS High Sierra IOHIDFamily 内存破坏漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：https://support.apple.com/zh-cn/HT208465
CNVD-2018-03422	多款 Huawei 产品 eSap software platform 堆缓冲区溢出漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：http://www.huawei.com/en/psirt/security-advisories/hw-345171
CNVD-2018-03436	Apple iOS/watchOS/tvOS/macOS High Sierra 内存破坏漏洞	高	目前厂商已发布升级补丁以修复漏洞，补丁获取链接：

			https://support.apple.com/zh-cn/HT201222

小结：本周，Jiangmin 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。此外，Apache、Extreme Networks、Linux 等多款产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、发起拒绝服务攻击或提升权限等。另外，Joomla!被披露存在 SQL 注入漏洞，攻击者可利用该漏洞危及应用程序，访问或修改数据，或利用底层数据库中潜在的漏洞。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. 超过 50000 个婴儿监视器被爆漏洞

最近，奥地利安全咨询公司（SEC Consult）的研究人员发现了 Mi-Cam 婴儿监视器中一组关键漏洞，超过 52,000 个婴儿监视器和用户帐户易受到攻击。利用这些漏洞，攻击者可以任意访问这些设备，并在没有进行身份认证的情况下打开一个视频流监视儿童。研究人员表示，这些婴儿监视器中使用的软件已经过时，并且存有不少广为人知的漏洞。自 2017 年 12 月以来 SEC Consult 多次通知 MiSafes 设备安全性问题，但该公司未做出任何回应。

参考链接：https://www.easyaq.com/news/1600883155.shtml

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：010-82991537