

信息安全漏洞周报

2017 年 11 月 27 日-2017 年 12 月 03 日

2017 年第 49 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 473 个，其中高危漏洞 174 个、中危漏洞 278 个、低危漏洞 21 个。漏洞平均分为 6.20。本周收录的漏洞中，涉及 0day 漏洞 95 个（占 20%），其中互联网上出现“Joomla! NS Download Shop 组件 SQL 注入漏洞、PHP CityPortal SQL 注入漏洞”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 698 个，与上周（509 个）环比增长 37%。

CNVD收录漏洞近10周平均分分布图

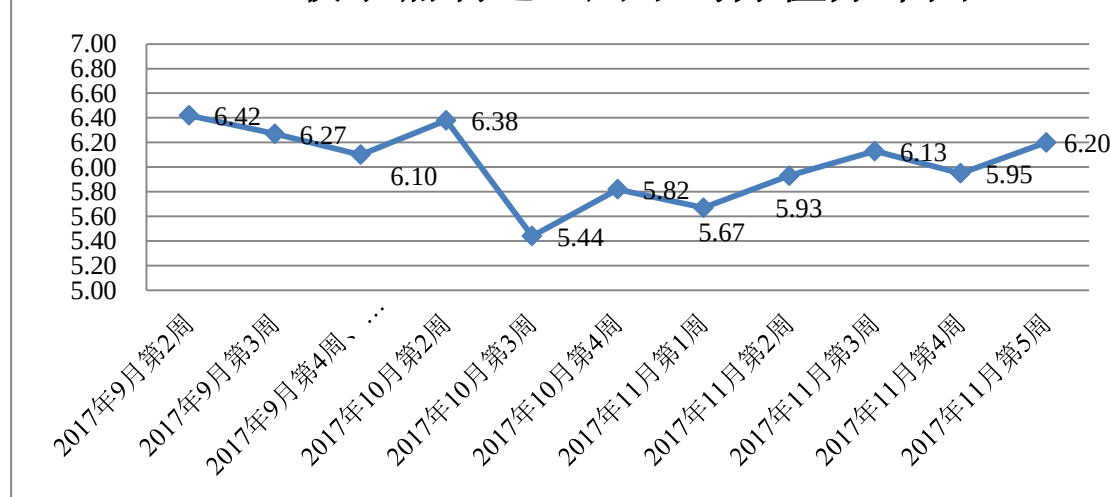


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周报送情况如表 1 所示。其中，安天实验室、绿盟科技、天融信、华为技术有限公司、H3C 等单位报送数量较多。深圳市鼎安天下信息科技有限公司、四川虹微技术有限公司（子午攻防实验室）、中新网络信息安全股份有限公司、网信智安、福建省海峡

信息技术公司、君立华域、漏斗社区、福建榕基软件股份有限公司、南京联成科技发展有限公司、爱加密、福建省海峡信息技术有限公司、聚锋信息安全实验室及其他个人白帽子向 CNVD 提交了 698 个以事件型漏洞为主的原创漏洞。

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
安天实验室	221	0
绿盟科技	195	0
天融信	190	2
360 网神	161	161
华为技术有限公司	173	0
漏洞盒子	127	127
H3C	98	0
恒安嘉新	73	0
启明星辰	70	0
中国电信集团系统集成有 限责任公司	68	0
杭州安恒信息技术有限公 司	55	0
知道创宇	2	0
深圳市腾讯计算机系统有 限公司（玄武实验室）	1	1
深圳市鼎安天下信息科技 有限公司	25	25
四川虹微技术有限公司 （子午攻防实验室）	16	16
中新网络信息安全股份有 限公司	12	12
网信智安	6	6
福建省海峡信息技术公司	4	4
君立华域	4	4

漏斗社区	4	4
福建榕基软件股份有限公司	2	2
南京联成科技发展股份有限公司	2	2
爱加密	1	1
福建省海峡信息技术有限公司	1	1
聚锋信息安全实验室	1	1
CNCERT 山西分中心	10	10
CNCERT 湖南分中心	9	9
CNCERT 重庆分中心	8	8
CNCERT 江西分中心	8	8
CNCERT 上海分中心	5	5
CNCERT 天津分中心	3	3
CNCERT 福建分中心	2	2
CNCERT 新疆分中心	2	2
CNCERT 西藏分中心	1	1
CNCERT 安徽分中心	1	1
CNCERT 宁夏分中心	1	1
CNCERT 浙江分中心	1	1
个人	278	278
报送总计	1841	698

本周漏洞按类型和厂商统计

本周，CNVD 收录了 473 个漏洞。其中应用程序漏洞 325 个，web 应用漏洞 91 个，网络设备漏洞 41 个，安全产品漏洞 8 个，操作系统漏洞 7 个，数据库漏洞 1 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	325
web 应用漏洞	91
网络设备漏洞	41
安全产品漏洞	8
操作系统漏洞	7
数据库漏洞	1

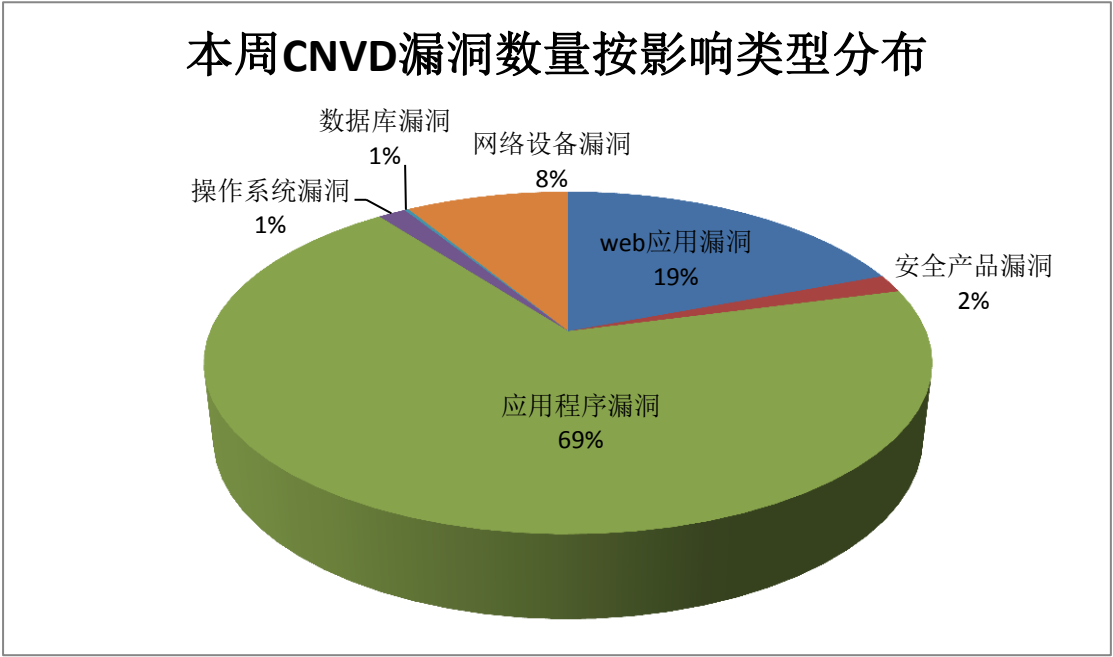


图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Adobe、Huawei、Cisco 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	Adobe	40	8%
2	Huawei	22	5%
3	Cisco	11	2%
4	WordPress	11	2%
5	EMC	8	2%
6	MediaWiki	7	1%
7	Google	7	1%
8	IBM	5	1%
9	Lenovo	4	1%
10	其他	358	77%

本周行业漏洞收录情况

本周，CNVD 收录了 25 个电信行业漏洞，85 个移动互联网行业漏洞，3 个工控行业漏洞（如下图所示）。其中，“多款 Cisco 产品远程代码执行漏洞、Huawei AR3200 整数溢出漏洞、D-Link DGS-1500 Ax 设备硬编码密码漏洞、Kabona AB WebDatorCentral 密码明文存储漏洞、Google Android Framework 权限提升漏洞(CNVD-2017-35660)”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/>

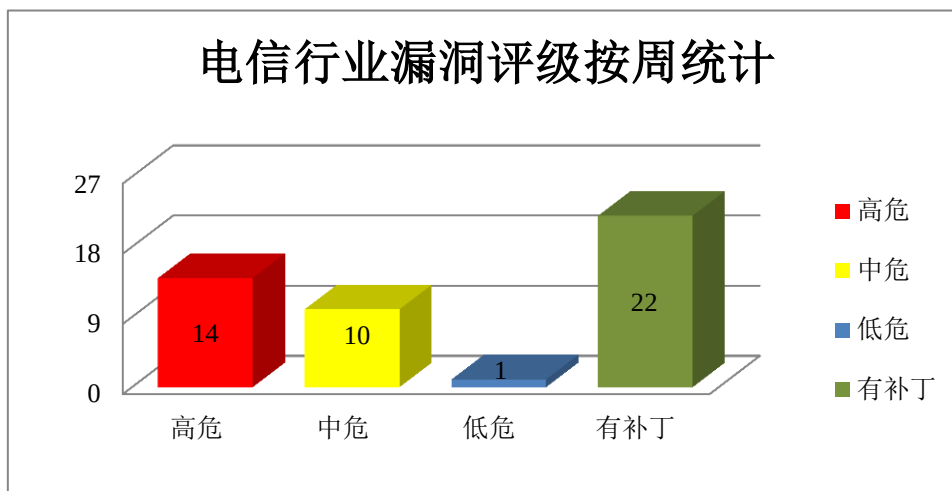


图 3 电信行业漏洞统计

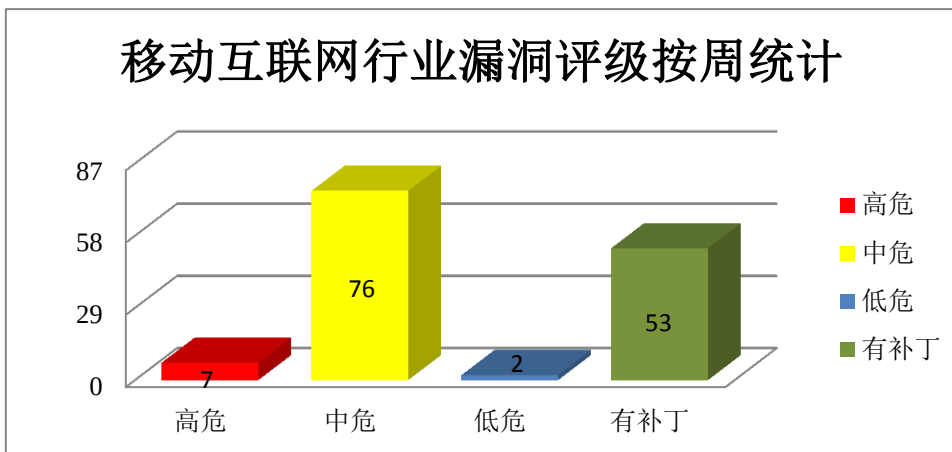


图 4 移动互联网行业漏洞统计

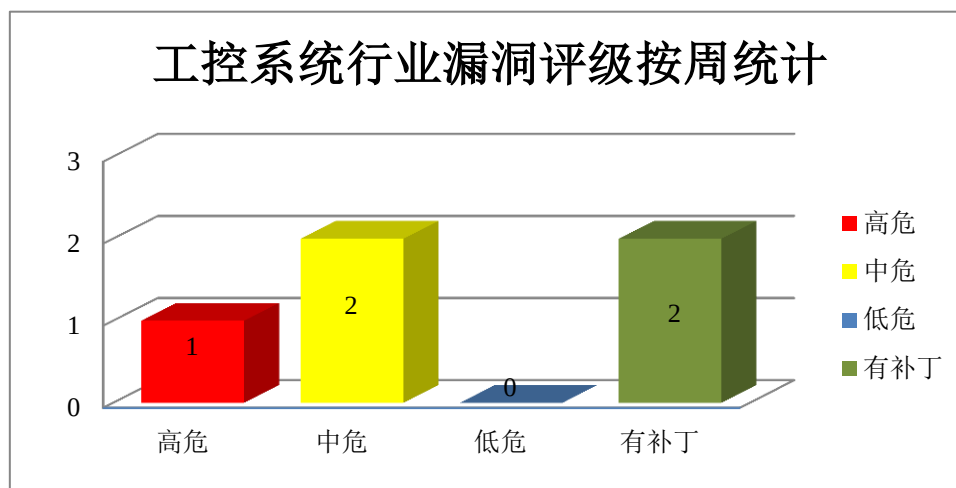


图 5 工控行业漏洞统计

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、Apache Struts2 存在多个漏洞

Struts2 是 Apache 软件基金会负责维护的一个基于 MVC 设计模式的 Web 应用框架开源项目。本周，上述产品被披露存在远程代码执行和反序列化漏洞，攻击者可利用漏洞对目标系统进行 Dos 攻击或反序列化代码执行攻击。

CNVD 收录的相关漏洞包括：Apache Struts2 S2-054 远程代码执行漏洞、FasterXML Jackson-databind 存在反序列化漏洞。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-2017-27693>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35898>

2、Adobe 产品安全漏洞

Adobe Reader 等都是美国奥多比（Adobe）公司的产品。Adobe Reader 是一款免费的 PDF 文件阅读器；Acrobat 是一款 PDF 文件编辑和转换工具；Acrobat Reader DC 是一套用于查看、打印和批注 PDF 的工具。本周，上述产品被披露存在远程代码执行漏洞，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 Acrobat 和 Reader 存在远程代码执行漏洞（CNVD-2017-35860、CNVD-2017-35861、CNVD-2017-35862、CNVD-2017-35863、CNVD-2017-35864、CNVD-2017-35865、CNVD-2017-35866、CNVD-2017-35867）。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-2017-35860>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35861>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35862>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35863>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35864>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35865>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35866>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35867>

3、Huawei 产品安全漏洞

Huawei AR3200 系列企业路由器是华为公司推出的新一代网络产品。Huawei TE40/50/60 是一款支持 1080p60 的高清视频会议终端。Huawei IPS Module 提供了由管理员、管理员界面组成的管理员机制。Huawei B2338-168 是一款能够接收 WiFi 信号的无线终端设备。Huawei P9 是一款智能手机。本周，上述产品被披露存在多个漏洞，攻击者可利用漏洞执行任意代码、提升权限或发起拒绝服务攻击等。

CNVD 收录的相关漏洞包括：Huawei AR3200 缓冲区溢出漏洞、Huawei AR3200 整数溢出漏洞、Huawei B2338-168 CPE 设备室外单元存在串口访问无认证漏洞、Huawei B2338-168 CPE 设备室外单元存在端口访问无认证漏洞、Huawei P9 权限提升漏洞、多款 Huawei 产品拒绝服务漏洞（CNVD-2017-35588、CNVD-2017-35593）、多款 Huawei 产品输入验证漏洞。除“Huawei P9 权限提升漏洞、多款 Huawei 产品拒绝服务漏洞（CNVD-2017-35593）”外，其余漏洞的综合评级为“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-2017-35596>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35594>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35439>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35440>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35443>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35588>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35593>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35589>

4、Cisco 产品安全漏洞

Cisco WebEx Business Suite（WBS30）client 等都是美国思科公司的视频会议解决方案的客户端软件。Cisco AMP for Endpoints 是高级恶意软件保护解决方案。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、提升权限、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：Cisco Aironet 认证绕过漏洞、Cisco AMP for Endpoints 本地权限提升漏洞、多款 Cisco 产品拒绝服务漏洞（CNVD-2017-35721）、多款 Cisco

co 产品远程代码执行漏洞、多款 Cisco 产品远程代码执行漏洞（CNVD-2017-35723、CNVD-2017-35724、CNVD-2017-35725、CNVD-2017-35726）。除“Cisco Aironet 认证绕过漏洞、Cisco AMP for Endpoints 本地权限提升漏洞、多款 Cisco 产品拒绝服务漏洞（CNVD-2017-35721）”外，其余漏洞的综合评级为“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-2017-35878>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35151>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35721>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35722>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35723>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35724>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35725>

<http://www.cnvd.org.cn/flaw/show/CNVD-2017-35726>

5、多款 ASUS 产品 networkmap 缓冲区溢出漏洞（CNVD-2017-35393）

ASUS RT-AC5300 等都是华硕（ASUS）公司的无线路由器。本周，ASUS 被披露存在缓冲区溢出漏洞，远程攻击者可利用该漏洞在路由器上执行任意代码。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-2017-35393>

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-2017-35302	Bitdefender Total Security 本地代码执行漏洞	高	用户可联系供应商获得补丁信息： http://www.bitdefender.com/
CNVD-2017-35375	Lhaz+不可信的搜索路径漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://chitora.com/jvn21369452.html
CNVD-2017-35389	Digital Arts i-filter 不可信的搜索路径漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.daj.jp/cs/info/2017/0912/
CNVD-2017-35391	Digital Arts i-filter 不可信的搜索路径漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.daj.jp/cs/info/2017/0912/
CNVD-2017-35654	Dulwich 任意命令执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.dulwich.io/code/dulwich/
CNVD-2017-35658	WebKit 和 WebKitGTK+远程代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新：

			http://trac.webkit.org/changeset/217126/webkit
CNVD-2017-35681	Computerinsel Photoline 代码执行漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://www.pl32.com/
CNVD-2017-35802	libpcap 设计漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.tcpdump.org/
CNVD-2017-35893	D-Link DGS-1500 Ax 设备硬编码密码漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： http://www.dlink.com.cn/
CNVD-2017-35894	Thornberry Ndoc 信息泄露漏洞	高	厂商已发布了漏洞修复程序，请及时关注更新： https://ndocsoftware.com/

表 4 部分重要高危漏洞列表

小结：本周，Apache Struts2 被披露存在远程代码执行和反序列化漏洞，攻击者可利用漏洞对目标系统进行 Dos 攻击或反序列化代码执行攻击。此外，Adobe、Huawei、Cisco 等多款产品被披露存在多个漏洞，攻击者可利用漏洞提升权限、执行任意代码或发起拒绝服务攻击等。另外，ASUS 被披露存在缓冲区溢出漏洞，远程攻击者可利用该漏洞在路由器上执行任意代码。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. Apache Struts2 再爆漏洞(ST2-054, ST2-055)

2017 年 12 月 1 日，Apache Struts 发布漏洞编号为 CVE-2017-15707（S2-054）和 CVE-2017-7525（S2-055）的安全漏洞，漏洞危害程度为中等（Moderate）。前者由于 Apache Struts REST 插件使用了过时的 JSON-lib 库，这个库很容易受到攻击，攻击者可以通过构造特制的 JSON 恶意请求造成 DOS 攻击；后者由于 Apache Struts 调用了存在反序列化漏洞的 Jackson JSON 库，导致了反序列化漏洞的产生。

参考链接：https://mp.weixin.qq.com/s/6tpylVO28g4mrb_15gkTdA

2. 关于 Intel ME SA-00086 漏洞

2017 年 11 月 20 日，Intel 官方发布了一则 Intel 多款固件安全更新公告(编号 Intel-SA-00086)。此公告提供了包括 Intel® Management Engine (ME), Intel® Server Platform Services (SPS), and Intel® Trusted Execution Engine (TXE)的安全漏洞情况和更新补丁。受影响的产品可能导致攻击者可以通过模拟 ME/SPS/TXE，危害本地安全特性认证的有效性；在用户和操作系统的可见性之外加载和执行任意代码；导致系统崩溃或系

统不稳定。

参考链接: <http://www.freebuf.com/news/154925.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: 010-82991537