

信息安全漏洞周报

2013 年 12 月 16 日-2013 年 12 月 22 日

2013 年第 51 期

本周漏洞基本情况

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 228 个，其中高危漏洞 53 个、中危漏洞 144 个、低危漏洞 31 个。上述漏洞中，可利用来实施远程攻击的漏洞有 209 个。本周收录的漏洞中，已有 189 个漏洞由厂商提供了修补方案，建议用户及时下载补丁更新程序，避免遭受网络攻击。本周互联网上出现“osCMax 任意文件上传漏洞”、“Telmanik CMS 'photo_upload.php'任意文件上传漏洞”等零日攻击代码，请使用相关产品的用户注意加强防范。

成员单位报送漏洞统计

本周，共 7 家成员单位、合作伙伴、国家互联网应急中心及个人报送了本周收录的全部 228 个漏洞。报送情况如表 1 所示。其中，安天实验室、启明星辰、天融信等单位报送数量较多。此外，国家互联网应急中心、High-Tech Bridge Security Research Lab、上海交通大学、中国电力科学研究院及个人报送者向 CNVD 提交了 11 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
安天实验室	138	0
启明星辰	116	0
天融信	92	0
绿盟	53	0
恒安嘉新	8	0
知道创宇	2	0
奇虎 360	1	0

国家互联网应急中心	3	3
High-Tech Bridge Security Research Lab	1	1
上海交大	2	2
中国电力科学研究院	2	2
个人	3	3
报送总计	421	11
录入总计	228（去重）	11

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 IBM、Cisco、FFmpeg 等多家厂商的产品，部分漏洞数量按厂商统计如表 2 所示。

序号	厂商（产品）	漏洞数量	所占比例
1	IBM	30	13%
2	Cisco	22	10%
3	FFmpeg	18	8%
4	Apple	10	4%
5	TYPO3	10	4%
6	Linux	6	3%
7	Wordpress	6	3%
8	SAP	6	3%
9	Red Hat	5	2%
10	其它	115	50%

表 2 漏洞产品涉及厂商分布统计表

漏洞按影响类型统计

本周，CNVD 收录了 228 个漏洞。其中应用程序漏洞 151 个，WEB 应用漏洞 45 个，操作系统漏洞 14 个，网络设备漏洞 11 个，安全产品漏洞 5 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	151
WEB 应用漏洞	45
网络设备漏洞	11
操作系统漏洞	14
安全产品漏洞	5
数据库系统漏洞	2

表 3 漏洞按影响类型统计表

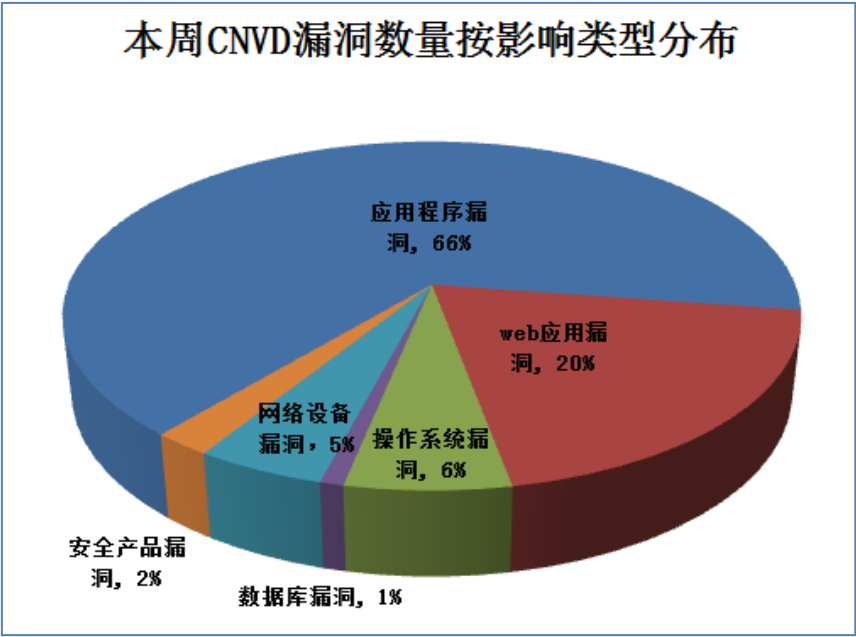


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 23 个电信行业漏洞、5 个移动互联网行业漏洞和 2 个工控系统漏洞（如下列表所示）。其中，“EMC Connectrix Manager Converged Network Edition 存在多个远程代码执行漏洞、Beetel Connection Manager 'NetConfig.ini'文件处理远程缓冲区溢出漏洞、D-Link DSR 路由器远程任意命令执行漏洞、MIUI 系统存在多个漏洞、WAGO PLC 无效指令处理拒绝服务漏洞”的综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-15051	D-Link DSL-6740U 跨站请求伪造漏洞	中	是
电信	CNVD-2013-15073	NowSMS Now SMS & MMS Gateway 拒绝服务漏洞	中	是
电信	CNVD-2013-15072	NowSMS Now SMS & MMS Gateway 拒绝服务漏洞（CNVD-2013-15072）	中	是
电信	CNVD-2013-15095	Cisco Scientific Atlanta D20 D30 cable modems 跨站脚本漏洞	中	是
电信	CNVD-2013-15156	Linksys Router 未授权管理访问漏洞	中	是
电信	CNVD-2013-15244	EMC Connectrix Manager Converged Network Edition 存在多个远程代码执行漏洞	高	是
电信	CNVD-2013-15238	Beetel Connection Manager	高	否

		'NetConfig.ini'文件处理远程缓冲区溢出漏洞		
电信	CNVD-2013-15237	D-Link DSR 路由器远程任意命令执行漏洞	高	是
电信	CNVD-2013-15272	HP LaserJet Printers CVE-2013-6193 未明远程拒绝服务漏洞	中	是
电信	CNVD-2013-15271	IBM Sterling Connect:Enterprise 存在未明跨站脚本漏洞	中	是
电信	CNVD-2013-15270	IBM WebSphere Service Registry 和 Repository HTML 注入漏洞	低	是
电信	CNVD-2013-15263	IBM Maximo Asset Management/SmartCloud Control Desk 产品多个跨站脚本漏洞	低	是
电信	CNVD-2013-15262	IBM DB2 / DB2 Connect XLST 库空指针引用拒绝服务漏洞	低	是
电信	CNVD-2013-15261	IBM DB2 / DB2 Connect OLAP 查询拒绝服务漏洞	低	是
电信	CNVD-2013-15291	Beetel TC1-450 Wireless Router 存在多个跨站请求伪造漏洞	低	否
电信	CNVD-2013-15289	Cisco EPC3925 Router 'Quick_setup'跨站请求伪造漏洞	低	否
电信	CNVD-2013-15307	D-Link DAP-2553 存在多个漏洞	中	是
电信	CNVD-2013-15378	Cisco ONS 15454 Transport Node Controller 远程拒绝服务漏洞	中	是
电信	CNVD-2013-15415	Trend Micro InterScan VirusWall 未授权代理连接漏洞	中	是
电信	CNVD-2013-15438	IBM Lotus iNotes 存在未明跨站脚本漏洞（CNVD-2013-15438）	中	是
电信	CNVD-2013-15444	Cisco NX-OS CLI 本地任意文件访问漏洞	中	是
电信	CNVD-2013-15445	IBM Lotus iNotes E-mail 消息未明存在 HTML 注入漏洞	中	是
电信	CNVD-2013-15446	IBM Lotus iNotes 存在未明 HTML 注入漏洞	低	是
移动互联网	CNVD-2013-15048	MIUI 系统存在多个漏洞	高	否
移动互联网	CNVD-2013-15052	Google Android 架构 Fragment 注入本地安全绕过漏洞	中	是
移动互联网	CNVD-2013-15073	NowSMS Now SMS & MMS Gateway 拒绝服务漏洞	中	是
移动	CNVD-2013-15072	NowSMS Now SMS & MMS Gateway	中	是

互联网		拒绝服务漏洞（CNVD-2013-15072）		
移动互联网	CNVD-2013-15276	Cisco WebEx Meeting Center 移动设备浏览器重定向跨站脚本漏洞	中	是
工控系统	CNVD-2013-15108	WAGO PLC 无效指令处理拒绝服务漏洞	高	否
工控系统	CNVD-2013-15287	Ecava IntegraXor 项目目录信息泄露漏洞	中	否

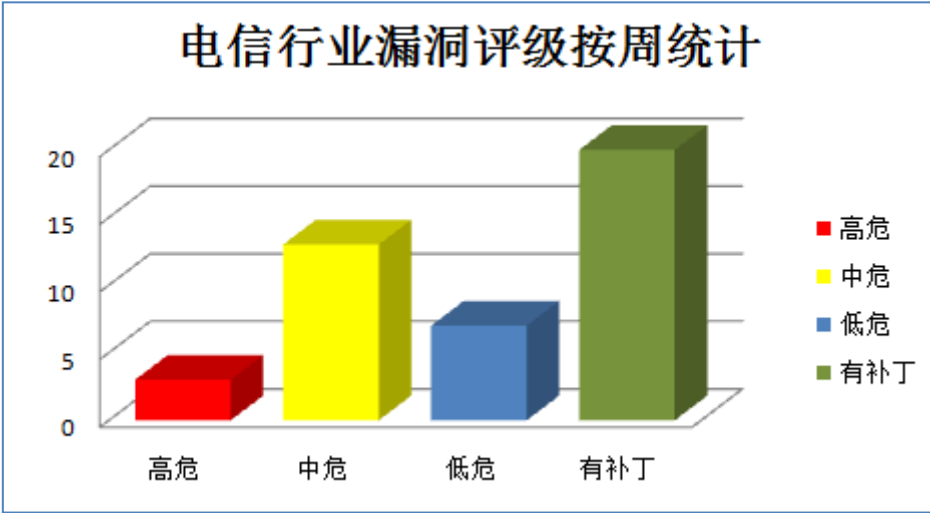


图 1 电信行业漏洞统计

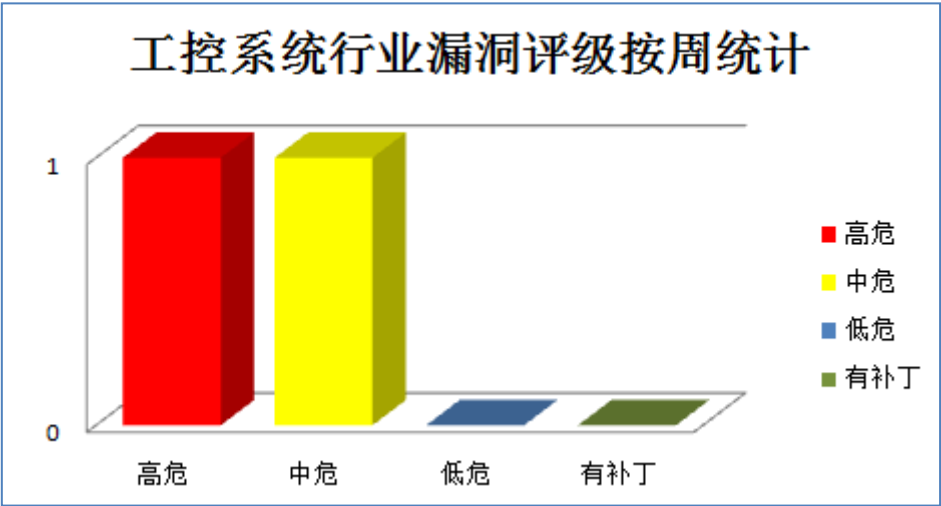


图 2 工控系统行业漏洞统计

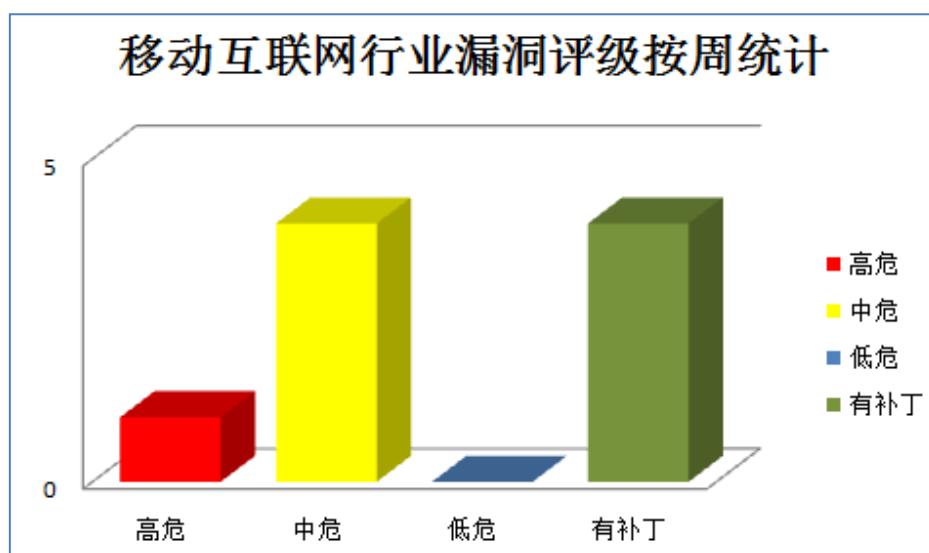


图 3 移动互联网行业漏洞统计

本周重要漏洞信息

本周，CNVD 整理和发布以下重要安全漏洞信息。

1、IBM 产品安全漏洞

IBM iNotes 是一个 Web 解决方案；IBM SPSS Collaboration and Deployment Service 是一款实时预测分析应用程序，包括模型部署，模型配置，数据采集，实时预测，模型性能监控，日志信息等；IBM Cognos 是一款集成商业智能（BI）和计划的解决方案。本周，上述产品被披露存在多个安全漏洞，攻击者利用漏洞可劫持用户会话，获得敏感信息。

CNVD 收录的相关漏洞包括：IBM Lotus iNotes 存在未明跨站脚本漏洞（CNVD-2013-15438）、IBM Lotus iNotes E-mail 消息未明存在 HTML 注入漏洞、IBM SPSS Collaboration and Deployment 密码泄露漏洞、IBM SPSS Collaboration and Deployment 开放重定向漏洞、IBM SPSS Collaboration and Deployment 跨站脚本漏洞、IBM SPSS Collaboration and Deployment 日志信息泄露漏洞、IBM Cognos Command Center 会话固定漏洞、IBM Cognos Command Center 会话固定漏洞等。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安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15438>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15445>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15361>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15363>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15372>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15373>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15255>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15246>

2、Red Hat 产品安全漏洞

Red Hat Enterprise MRG 是一款 Redhatlinux 发行的即时通信网络解决方案。本周，该产品被披露存在多个安全漏洞，攻击者利用漏洞可劫持用户会话，获得敏感数据库信息。

CNVD 收录的相关漏洞包括：Red Hat Enterprise MRG Cumin 存在未明 SQL 注入漏洞、Red Hat Enterprise MRG Cumin 非特权用户安全绕过漏洞、Red Hat Enterprise MRG Cumin Web Interface 跨站脚本漏洞、Red Hat Enterprise MRG Cumin WEB 接口存在多个跨站请求伪造漏洞、Red Hat JBoss Portal GateIn Portal 不正确 URL 转义存在多个反射型跨站脚本漏洞。其中，“Red Hat Enterprise MRG Cumin 存在未明 SQL 注入漏洞”的综合评级均“高危”。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安全事件。

参考链接：<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15442>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15439>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15441>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15443>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15365>

3、Apple 产品安全漏洞

Apple Safari 是一款 WEB 浏览器。本周，该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，执行任意代码。

CNVD 收录的相关漏洞包括：Apple Safari For Windows 远程代码执行漏洞、Apple Safari 存在多个跨域信息泄露漏洞、Apple Safari LastSession.plist 信息泄露漏洞。厂商已经发布了“Apple Safari 存在多个跨域信息泄露漏洞”的修补程序。CNVD 提醒用户尽快下载补丁更新，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-2013-15381>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15347>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15382>

4、Cisco 产品安全漏洞

Cisco WebEx Training Center 是一个在线培训解决方案。本周，该产品被披露存在多个漏洞，攻击者利用漏洞可获得敏感信息，发起网络钓鱼攻击。

CNVD 收录的相关漏洞包括：Cisco WebEx Training Center Training Registration 页面内容欺骗漏洞、Cisco WebEx Training Center 存在多个信息泄露漏洞、Cisco WebEx Training Center email 枚举漏洞、Cisco WebEx Training Center 注册 ID 泄露漏洞、Cisco WebEx Training Center 培训会会话号信息泄露漏洞、Cisco WebEx Training Center 开放重定

向漏洞（CNVD-2013-15317、CNVD-2013-15318）、Cisco WebEx Training Center Email 验证绕过音频会议加入漏洞等。厂商已发布了上述漏洞的修补程序。CNVD 提醒相关用户尽快下载补丁更新，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-2013-15264>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15273>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15314>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15315>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15316>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15317>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15318>
<http://www.cnvd.org.cn/flaw/show/CNVD-2013-15319>

5、osCMax 任意文件上传漏洞

osCMax 是一套基于 PHP 的开源电子商务系统、购物车应用程序。本周，osCMax 被披露存在一个综合评级为“高危”的文件上传漏洞，远程攻击者利用漏洞可上传任意文件。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-2013-15430>

更多高危漏洞如表 3 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-2013-15437	EMC RSA Archer GRC 存在多个未明跨站脚本漏洞（CNVD-2013-15437）	高	RSA Archer GRC 5.4 P2 或 5.4 SP1 已经修复该漏洞，建议用户下载更新： https://knowledge.rsasecurity.com
CNVD-2013-15428	Auction Website Script Ebay Clone'id'参数 SQL 注入漏洞	高	暂无
CNVD-2013-15432	Veno File Manager 任意文件下载漏洞	高	暂无
CNVD-2013-15433	RealPlayer 'RMP'文件处理远程堆缓冲区溢出漏洞	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： http://www.real.com/realplayer
CNVD-2013-15367	Iscripts supportdesk 存在多个 SQL 注入漏洞	高	暂无

CNVD-2013-15357	IrfanView Formats PlugIn 'MrSID.dll' 'levels'头解析远程任意代码执行漏洞	高	IrfanView Formats PlugIn 4.37 已经修复该漏洞，建议用户下载更新： http://www.irfanview.com
CNVD-2013-15369	Icinga Web GUI 多个单字节溢出内存破坏漏洞	高	Icinga 1.10.2, 1.9.4, 1.8.5 已经修复该漏洞，建议用户下载更新： https://dev.icinga.org/issues/5251
CNVD-2013-15279	SAP Customer Relationship Management XML 外部实体注入漏洞	高	用户可参考如下厂商提供的安全公告获得补丁信息： https://service.sap.com/sap/support/notes/1909665
CNVD-2013-15267	Telmanik CMS 'photo_upload.php' 任意文件上传漏洞	高	暂无
CNVD-2013-15117	TYPO3 OpenID Extension 存在未明任意站点重定向漏洞	高	TYPO3 4.5.32, 4.7.17, 6.0.12, 6.1.7 已经修复该漏洞，建议用户下载更新： http://typo3.org/

表 3 部分高危漏洞列表

小结：Apple Safari、Red Hat Enterprise MRG、Cisco WebEx Training Center 和 IBM 多款产品被披露存在多个漏洞，攻击者利用漏洞可劫持用户会话，获得敏感信息，执行任意代码。此外，osCMax 应用程序被披露存在一个高危零日漏洞，建议相关用户应随时关注厂商主页，及时获取修复补丁或解决方案。

本周重要漏洞修补信息

CNVD 整理和发布以下重要安全修补信息。

1、D-Link 修补多款产品漏洞

D-Link DAP-2553 和 D-Link DSL-6740U 是一款路由器设备；D-Link DSR 是无线服务路由器产品。本周，D-Link 修补了上述产品存在的多个漏洞，避免攻击者利用漏洞获取敏感信息，以 root 用户权限执行任意命令。CNVD 已收录相关补丁，请广大用户及时下载更新，避免引发漏洞相关的安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/41826>

<http://www.cnvd.org.cn/patchInfo/show/41739>

<http://www.cnvd.org.cn/patchInfo/show/41671>

本周要闻速递

1. 新漏洞能激活苹果 iSight 摄像头

近日有消息报道，Johns Hopkins 大学研究人员发现了针对 Macbook 和 iMac 的新攻击手段，通过输入定制的固件能够在无需打开相机随附的 LED 灯光的情况下激活 iSight 摄像头进行拍摄。苹果 iSight 摄像头系统采用了名为“hardware interlock”（硬件互锁）

的技术让摄像头传感器和内置 LED 进行捆绑，而且 LED 直接链接到传感器上，所以两者的开启和关闭都属于同一个状态。然而，研究人员重新对 iSight 摄像头的固件进行了重新编写，使之在经过 USB 端口等进行的通讯的时候绕过“硬件互锁”，能够在 LED 灯光在不开启的情况下激活摄像头进行拍摄，这表明潜在的攻击完全可以通过这种手段存在，从而威胁到用户的个人隐私。

参考链接：<http://notebook.it168.com/a2013/1223/1576/000001576969.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

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 1999 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截止 2012 年，CNCERT 与 51 个国家和地区的 91 个组织建立了“CNCERT 国际合作伙伴”关系。

网址：www.cert.org.cn

邮箱：vreport@cert.org.cn

电话：010-82990999