

信息安全漏洞周报

2014 年 11 月 17 日-2014 年 11 月 23 日

2014 年第 47 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**低**。

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 138 个，其中高危漏洞 43 个、中危漏洞 84 个、低危漏洞 11 个。上述漏洞中，可利用来实施远程攻击的漏洞有 120 个。本周收录的漏洞中，已有 104 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“Piwigo 'rate'参数 SQL 注入漏洞”、“多款 Magento 产品任意文件上传漏洞”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 家成员单位及个人报送了本周收录的全部 138 个漏洞。报送情况如表 1 所示。其中，恒安嘉新、安天实验室、天融信、启明星辰等单位报送数量较多。此外，CNCERT 各分中心、北京数字认证股份有限公司及白帽子向 CNVD 提交了 49 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
恒安嘉新	134	0
安天实验室	111	0
天融信	110	0
启明星辰	85	0
绿盟科技	48	0
奇虎	2	2

北京数字认证股份有限公司	1	1
CNCERT 江西分中心	14	14
CNCERT 福建分中心	13	13
CNCERT 山西分中心	13	13
CNCERT 河南分中心	1	1
CNCERT 黑龙江分中心	1	1
CNCERT 新疆分中心	1	1
个人	3	3
报送总计	537	49
录入总计	138（去重）	49

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Moodle、Google、IBM 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	Moodle	15	11%
2	Google	13	9%
3	IBM	8	6%
4	Apple	8	6%
5	Linux	6	4%
6	WordPress	5	4%
7	Cisco	5	4%
8	Wireshark	5	4%
9	GoGits	3	2%
10	其他	70	50%

表 2 漏洞产品涉及厂商分布统计表

本周，CNVD 收录了 138 个漏洞。其中应用程序漏洞 83 个，WEB 应用漏洞 26 个，操作系统漏洞 18 个，网络设备漏洞 11 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	83
WEB 应用漏洞	26
操作系统漏洞	18
网络设备漏洞	11

表 3 漏洞按影响类型统计表

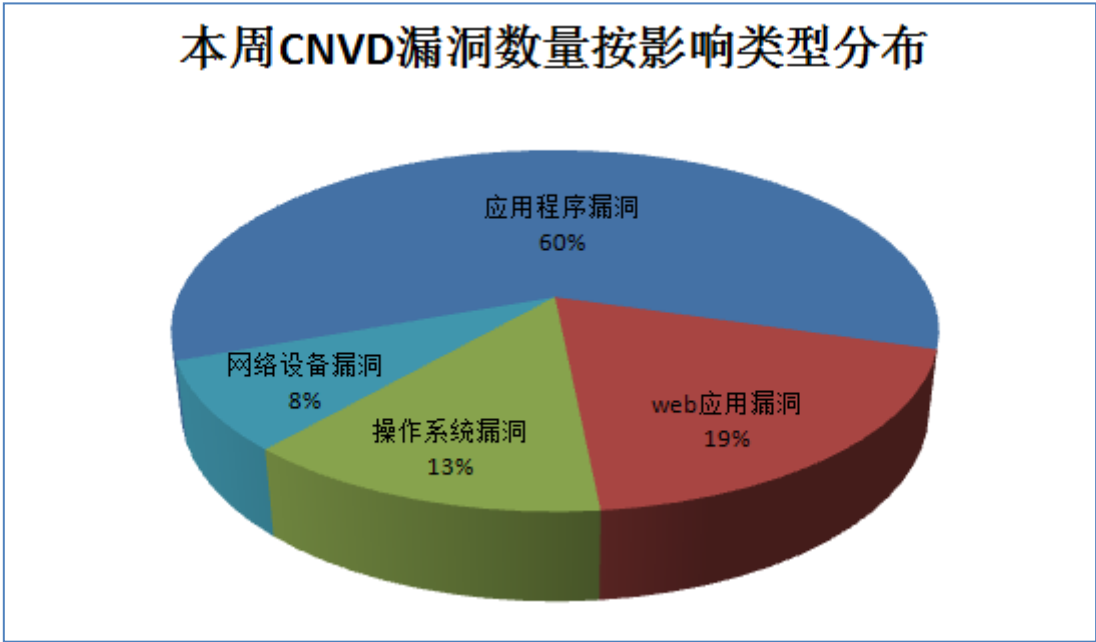


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 10 个电信行业漏洞，9 个移动互联网漏洞，2 个工控系统行业漏洞（如下图表所示）。其中，“Check Point Security Gateways 拒绝服务漏洞（CNVD-2014-08326、CNVD-2014-08327、CNVD-2014-08328）、Apple iOS and TV 远程代码执行漏洞、Apple iOS Lock Screen 安全绕过漏洞（CNVD-2014-08375）、Apple iOS 二进制文件执行限制绕过漏洞、Google Android 本地权限提升漏洞、Rockwell Automation Connected Components Workbench 存在多个任意代码执行漏洞、Advantech WebAccess 栈缓冲区溢出漏洞”的综合评级均为“高危”。相关厂商已经发布了上述漏洞的修补程序。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2014-08309	ZTE 831CII 存在多个漏洞	中	否
电信	CNVD-2014-08326	Check Point Security Gateways 拒绝服	高	是

		务漏洞（CNVD-2014-08326）		
电信	CNVD-2014-08327	Check Point Security Gateways 拒绝服务漏洞（CNVD-2014-08327）	高	是
电信	CNVD-2014-08328	Check Point Security Gateways 拒绝服务漏洞（CNVD-2014-08328）	高	是
电信	CNVD-2014-08350	Cisco IOS 信息泄露漏洞（CNVD-2014-08350）	中	否
电信	CNVD-2014-08366	Cisco Aironet Access Points DHCP Subsystem 拒绝服务漏洞	中	是
电信	CNVD-2014-08365	Cisco Aironet Access Points 拒绝服务漏洞	中	是
电信	CNVD-2014-08404	多款 Samsung Galaxy 设备 KNOX 任意代码执行漏洞	高	否
电信	CNVD-2014-08397	Cisco Unified Communications Manager IM and Presence Service 信息泄露漏洞	中	否
电信	CNVD-2014-08428	ZTE ZXHN H108L Router 远程身份验证绕过漏洞	中	否
移动互联网	CNVD-2014-08338	Apple Mac OS X/iOS 信息泄露漏洞（CNVD-2014-08338）	中	是
移动互联网	CNVD-2014-08339	Apple Mac OS X/iOS 信息泄露漏洞（CNVD-2014-08339）	中	是
移动互联网	CNVD-2014-08371	Apple iOS and TV 远程代码执行漏洞	高	是
移动互联网	CNVD-2014-08376	Apple iOS Lock Screen 安全绕过漏洞（CNVD-2014-08376）	低	是
移动互联网	CNVD-2014-08374	Apple iOS and TV 本地代码执行漏洞	低	是
移动互联网	CNVD-2014-08375	Apple iOS Lock Screen 安全绕过漏洞（CNVD-2014-08375）	高	是
移动互联网	CNVD-2014-08398	Microsoft Windows Phone 本地权限提升漏洞	中	否
移动互联网	CNVD-2014-08415	Apple iOS 二进制文件执行限制绕过漏洞	高	是
移动互联网	CNVD-2014-08431	Google Android 本地权限提升漏洞	高	是
工控系统	CNVD-2014-08308	Rockwell Automation Connected Components Workbench 存在多个任意代码执行漏洞	高	是
工控系统	CNVD-2014-08420	Advantech WebAccess 栈缓冲区溢出漏洞	高	是

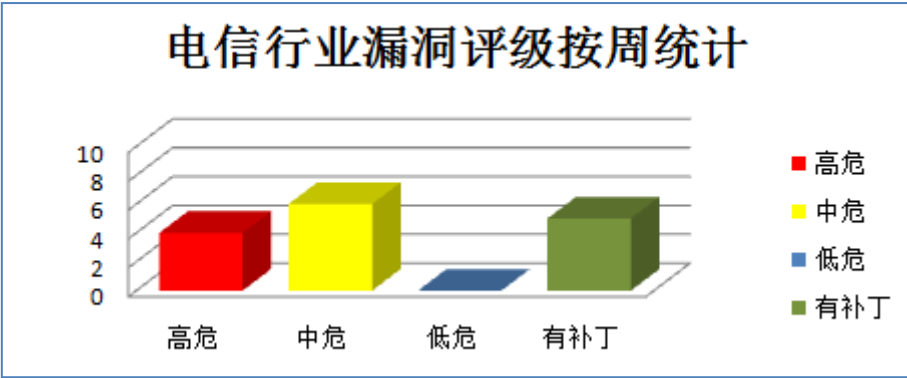


图 1 电信行业漏洞统计

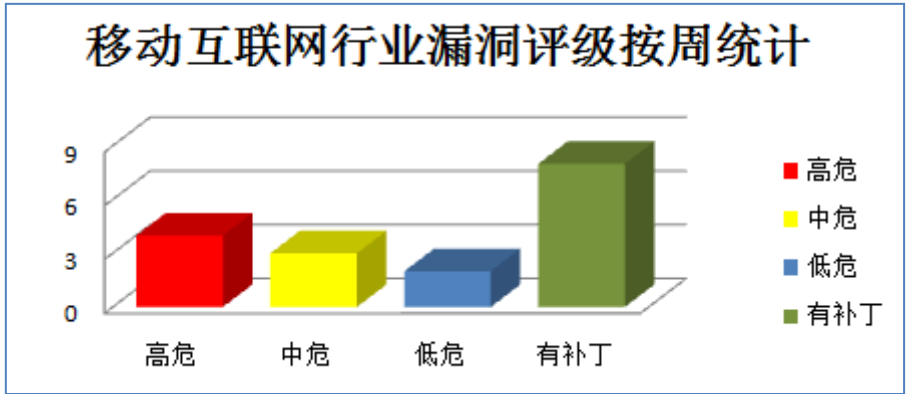


图 2 移动互联网行业漏洞统计

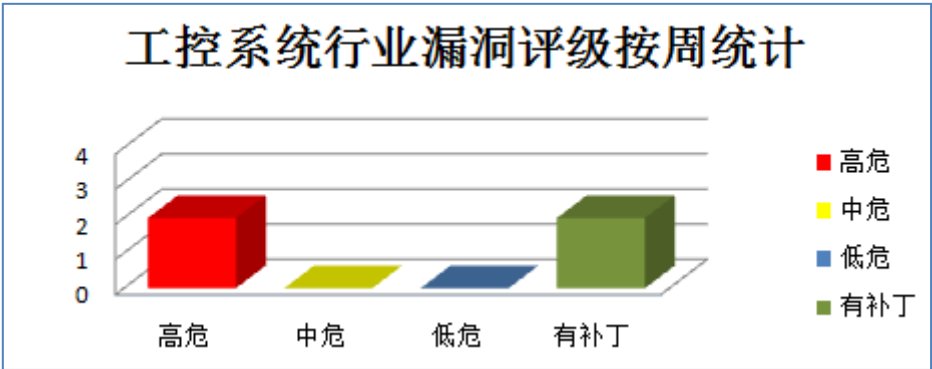


图 3 工控系统行业漏洞统计



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、Google 产品安全漏洞

Google Chrome 是由 Google 开发的一款 Web 浏览工具。本周，上述产品被披露存在内存错误引用远程代码执行漏洞、缓冲区溢出和整数溢出漏洞，攻击者可利用漏洞发起拒绝服务或执行任意代码。

CNVD 收录的相关漏洞包括：Google Chrome 整数溢出漏洞（CNVD-2014-08388、CNVD-2014-08389）、Google Chrome 内存错误引用远程代码执行漏洞（CNVD-2014-08384、CNVD-2014-08383、CNVD-2014-08382、CNVD-2014-08391）、Google Chrome 缓冲区溢出漏洞（CNVD-2014-08385、CNVD-2014-08386）。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-2014-08388>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08389>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08384>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08383>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08382>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08391>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08385>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08386>

2、Apple 产品安全漏洞

Apple iOS 是由苹果公司开发的移动操作系统。Apple Mac OS X 是一款苹果公司开发的电脑操作系统。Apple TV 是一款由苹果公司所设计、营销和销售的数字多媒体机。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、执行任意代码或进行未授权操作。

CNVD 收录的相关漏洞包括：Apple iOS 二进制文件执行限制绕过漏洞、Apple Mac OS X/iOS 信息泄露漏洞（CNVD-2014-08339、CNVD-2014-08338）、Apple iOS and TV 远程代码执行漏洞、Apple iOS Lock Screen 安全绕过漏洞（CNVD-2014-08375、CNVD-2014-08376）、Apple Mac OS X 信息泄露漏洞（CNVD-2014-08373）、Apple iOS and TV 本地代码执行漏洞。其中“Apple iOS 二进制文件执行限制绕过漏洞、Apple iOS and TV 远程代码执行漏洞、Apple iOS Lock Screen 安全绕过漏洞（CNVD-2014-08375）”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-2014-08415>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08339>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08338>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08371>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08375>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08376>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08373>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08374>

3、Moodle 产品安全漏洞

Moodle 是一款开放源代码的网络教学应用程序。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、执行任意代码、绕过安全限制或进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：Moodle 存在未明任意文件上传漏洞、Moodle LTI 模块安全绕过漏洞、Moodle 信息泄露漏洞（CNVD-2014-08355）、Moodle 'mod/feedback/mapcourse.php'跨站脚本漏洞、Moodle 'lib/phpunit/bootstrap.php'路径泄露漏洞、Moodle 弱口令漏洞、Moodle 'forum_get_discussions()'函数安全绕过漏洞、Moodle 'tag/tag_auto_complete.php'未授权访问漏洞。其中“Moodle 存在未明任意文件上传漏洞”的综合评级为“高危”。目前，厂商已经发布了修补程序。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-2014-08343>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08356>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08355>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08354>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08353>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08344>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08342>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08340>

4、IBM 产品安全漏洞

IBM Java SDK 是一款 Java 实现平台。IBM Security Identity Manager 是 IBM Security Systems 产品组合的一员，能帮助组织跨整个企业推动有效的身管理理与控管，减少身分诈骗风险并提升法规遵循。IBM Tivoli Storage Manager 是一款遵循 ANSI SAN 标准的可扩展解决方案，用于发现、监控和管理企业 SAN 架构组件，并可分配和自动操纵企业的附加磁盘存储资源。本周，上述产品被披露存在多个安全漏洞，攻击者可利用漏洞获取敏感信息、执行任意代码、执行未授权访问或进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：IBM Java SDK 本地任意代码执行漏洞、IBM Security Identity Manager 信息泄露漏洞（CNVD-2014-08349、CNVD-2014-08360）、IBM Security Identity Manager 点击劫持漏洞、IBM Security Identity Manager 目录遍历漏洞、IBM Security Identity Manager 跨站脚本漏洞、IBM Security Identity Manager 本地安全绕过漏洞、IBM Tivoli Storage Manager Server 本地未授权访问漏洞（CNVD-2014-08361）。目前，厂商已经发布了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-2014-08401>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08349>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08360>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08347>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08346>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08359>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08345>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-08361>

5、Joomla! HD FLV Player Component 'index.php' SQL 注入漏洞

Joomla!是一款开源的内容管理系统。本周，Joomla! HD FLV Player Component 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可利用漏洞危及受影响的应用程序，访问或修改数据库数据。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-2014-08316>

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-2014-08409	Vision HelpDesk 存在未明 SQL 注入漏洞	高	Vision HelpDesk 3.8.6 已经修复该漏洞，建议用户下载更新： http://www.thevisionworld.com/vision-helpdesk-v3-8-6-stable-version-released.html
CNVD-2014-08420	Advantech WebAccess 栈缓冲区溢出漏洞	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://webaccess.advantech.com/
CNVD-2014-08417	Aruba Networks ClearPass 任意命令执行漏洞	高	用户可参考如下供应商提供的安全公告获得补丁信息： http://www.arubanetworks.com/support/alerts/aid-10282014.txt
CNVD-2014-08412	Lsyncd 'default-rsyncssh.lua'远程命令注入漏洞	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： https://github.com/axkibe/lsyncd
CNVD-2014-08410	Faronics Deep Freeze Standard and Enterprise 'DfDiskLo.sys'本地任意代码执行漏洞	高	暂无
CNVD-2014-08425	GoGits Gogs 存在多个 SQL 注入漏洞	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://try.gogs.io/

CNVD-2014-08424	GoGits Gogs 'label'参数 SQL 注入漏洞	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://try.gogs.io/
CNVD-2014-08423	Dolibarr 存在多个 SQL 注入漏洞（CNVD-2014-08423）	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.dolibarr.org/
CNVD-2014-08422	Advantech AdamView 存在多个栈缓冲区溢出漏洞	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.advantech.com/
CNVD-2014-08421	Advantech EKI-6340 命令注入漏洞	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.advantech.com/

表 3 部分高危漏洞列表

小结：本周，Google Chrome 产品被批露存在内存错误引用远程代码执行漏洞、缓冲区溢出和整数溢出漏洞，攻击者可利用漏洞发起拒绝服务或执行任意代码。此外，Apple、Moodle、IBM 多款产品被批露存在多个安全漏洞，允许攻击者利用漏洞获取敏感信息、执行任意代码、发起拒绝服务和跨站脚本攻击或执行未授权操作。另外，Joomla! HD FLV Player Component 被披露存在一个高危零日漏洞。攻击者可利用漏洞危及受影响的应用程序，访问或修改数据库数据。建议相关用户应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、Microsoft 修补 Windows 产品漏洞

Microsoft Windows 是一款流行的操作系统。

本周，Microsoft 修补了上述产品存在的权限提升漏洞，避免攻击者利用漏洞获得域管理员权限。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网络安全事件。

补丁下载链接：<http://www.cnvd.org.cn/patchInfo/show/52039>

本周要闻速递

1. WordPress 4.0.1 发布 修复关键安全漏洞

WordPress3.9.2 及以下的版本包含一个严重的跨站脚本漏洞，可以让匿名的用户破坏网站，但是这个漏洞不会影响 4.0 版本。4.0.1 解决了 8 个安全问题，同时还修复了 23 个 bugs，还有两处重大的改进，包括更好的 EXIF 数据验证（从上传图片提取的）。

参考链接：<http://www.d1net.com/security/news/316762.html>

2. 苹果更新 Flash 网页浏览器插件并修复安全漏洞

苹果公司针对 Adobe 的 Flash Player 浏览器插件进行更新。本次更新修复了一个最近发现的 Adobe Flash Player 网页插件漏洞。当用户使用 Flash Player 来访问某个网页时，系统就会提示用户安装本次更新。此前苹果因为 Safari 浏览器 Java 插件漏洞，让公司内部 Mac 被病毒感染。后来苹果对 Safari 浏览器做出了一些改动，苹果 Safari 浏览器强制要求 Adobe Flash Player 更新。而在最新版本的 Safari 当中，苹果将会对未更新的插件进行系统封锁。也就是说最新版本的苹果 Safari 浏览器中，检测到你的 Adobe Flash Player 尚未更新还处于旧版本。那么系统就会封锁该插件，如果用户需要使用该插件必须更新后才能正常的观看有关 Flash 的内容。

参考链接：<http://news.cnfol.com/it/20141121/19518790.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：010-82990999