

信息安全漏洞周报

2014 年 8 月 18 日-2014 年 8 月 24 日

2014 年第 34 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 126 个，其中高危漏洞 34 个、中危漏洞 75 个、低危漏洞 17 个。上述漏洞中，可利用来实施远程攻击的漏洞有 114 个。本周收录的漏洞中，已有 90 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“ArticleFR 'id'参数 SQL 注入漏洞”、“WordPress 插件 CK and SyntaxHighlighter '/ckfinder/ckfinder.html'远程代码执行漏洞”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 6 家成员单位、合作伙伴及个人报送了本周收录的全部 126 个漏洞。报送情况如表 1 所示。其中，奇虎 360、安天实验室、绿盟科技、天融信、恒安嘉新等单位报送数量较多。此外，CNCERT 各分中心、High-Tech Bridge Security Research、习科网络安全及白帽子向 CNVD 提交了 438 个原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎 360	401	401
安天实验室	118	0
绿盟科技	99	0
天融信	96	0
恒安嘉新	92	0
启明星辰	74	0

习科网络安全	2	2
High-Tech Bridge Security Research	1	1
CNCERT 江西分中心	8	8
CNCERT 福建分中心	8	8
CNCERT 山西分中心	5	5
CNCERT 陕西分中心	1	1
CNCERT 上海分中心	1	1
个人	11	11
报送总计	917	438
录入总计	126（去重）	438

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、WordPress、EMC 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	17	13%
2	Wordpress	12	10%
3	EMC	9	7%
4	Apache	5	4%
5	Cisco	3	2%
6	Mathias Kettner	3	2%
7	FFmpeg	2	2%
8	Linux	2	2%
9	Red Hat	2	2%
10	其他	71	56%

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 126 个漏洞。其中应用程序漏洞 88 个，WEB 应用漏洞 27 个，网络设备漏洞 5 个，操作系统漏洞 4 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	88
WEB 应用漏洞	27

网络设备漏洞	5
操作系统漏洞	4
安全产品漏洞	2

表 3 漏洞按影响类型统计表

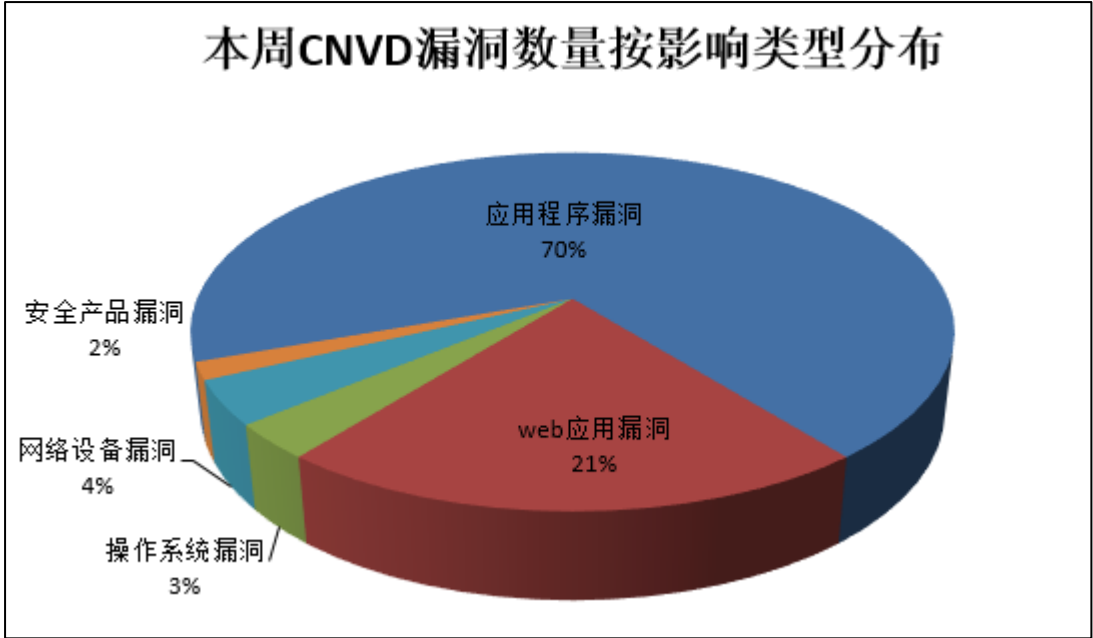


图 1 本周漏洞按影响类型分布

本周行业漏洞信息

本周，CNVD 收录了 11 个电信行业漏洞，3 个移动互联网漏洞，1 个工控行业漏洞（如下图表所示）。其中，“IBM WebSphere Application Server 拒绝服务漏洞（CNVD-2014-05174）、Siemens SIMATIC S7-1500 拒绝服务漏洞（CNVD-2014-05089）”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-2014-05054	IBM Tivoli Storage Manager 本地缓冲区溢出漏洞	低	是
电信	CNVD-2014-05055	IBM Tivoli Storage Manager 本地未授权访问漏洞	低	是
电信	CNVD-2014-05074	IBM WebSphere DataPower SOA Appliances 信息泄露漏洞	中	是
电信	CNVD-2014-05093	IBM Business Process Manager 文件读取漏洞	中	是
电信	CNVD-2014-05125	Tenda A5S 路由器 Cookie 身份验证绕过漏洞	高	否
电信	CNVD-2014-05130	Cisco ASR 5000 Series Software 拒绝服务漏洞	中	是

电信	CNVD-2014-05162	Huawei Campus Series Switches 用户枚举漏洞	中	是
电信	CNVD-2014-05170	IBM WebSphere Application Server 安全绕过漏洞 (CNVD-2014-05170)	中	是
电信	CNVD-2014-05171	IBM WebSphere Application Server 安全绕过漏洞 (CNVD-2014-05171)	低	是
电信	CNVD-2014-05172	IBM WebSphere Application Server 信息泄露漏洞 (CNVD-2014-05172)	中	是
电信	CNVD-2014-05174	IBM WebSphere Application Server 拒绝服务漏洞 (CNVD-2014-05174)	高	是
移动互联网	CNVD-2014-05065	BlackBerry 多个产品异常处理信息泄露漏洞 (CNVD-2014-05065)	中	是
移动互联网	CNVD-2014-05079	Ameba for Android SSL 证书验证欺骗漏洞	中	是
移动互联网	CNVD-2014-05127	PHP-sqlr 存在未明 SQL 注入漏洞	高	否
工控系统	CNVD-2014-05089	Siemens SIMATIC S7-1500 拒绝服务漏洞 (CNVD-2014-05089)	高	是

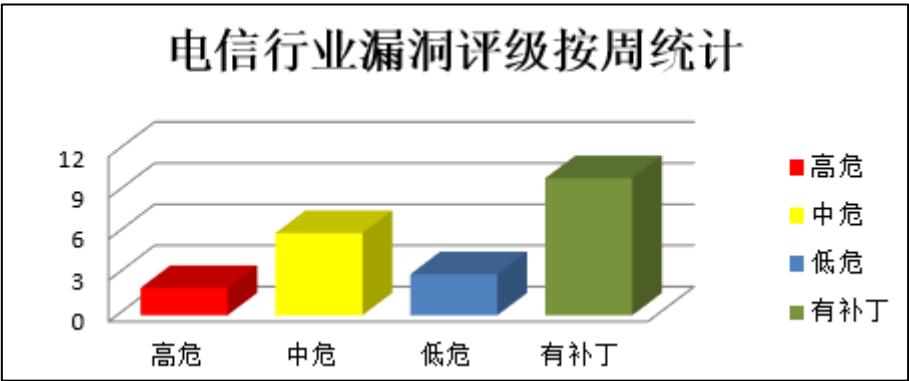


图 1 电信行业漏洞统计

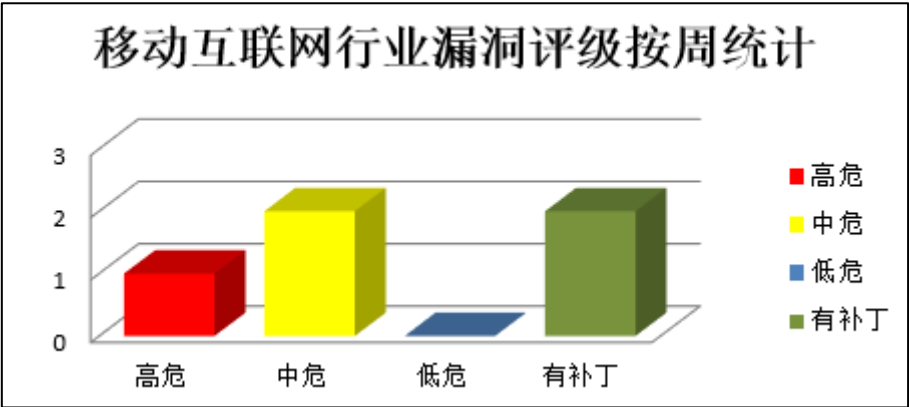


图 2 移动互联网行业漏洞统计

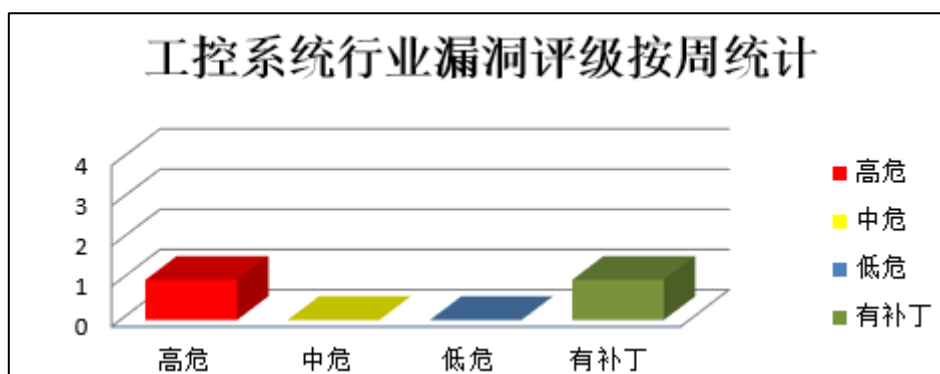


图 3 工控行业漏洞统计

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 WebSphere Application Server (WAS) 是美国 IBM 公司开发并发行的一款应用服务器产品，它是 Java EE 和 Web 服务应用程序的平台，也是 IBM WebSphere 软件平台的基础。IBM InfoSphere Master Data Management 是主数据管理解决方案。PowerVC 是 IBM 基本虚拟化管理的解决方案。IBM Business Process Manager 是一款不断积累数据的有状态产品。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、执行未经授权操作或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：IBM WebSphere Application Server 拒绝服务漏洞 (CNVD-2014-05174)、多个 IBM InfoSphere Master Data Management 产品本地权限提升漏洞、IBM InfoSphere Master Data Management Collaboration Server SQL 注入漏洞、IBM PowerVC 中间人攻击漏洞 (CNVD-2014-05154)、IBM WebSphere Application Server 信息泄露漏洞 (CNVD-2014-05172)、IBM WebSphere Application Server 安全绕过漏洞 (CNVD-2014-05170)、IBM Business Process Manager 文件读取漏洞、IBM InfoSphere Master Data Management 信息泄露漏洞。其中“IBM WebSphere Application Server 拒绝服务漏洞 (CNVD-2014-05174)、多个 IBM InfoSphere Master Data Management 产品本地权限提升漏洞、IBM InfoSphere Master Data Management Collaboration Server SQL 注入漏洞”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-2014-05174>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05102>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05101>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05154>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05172>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05170>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05093>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05092>

2、EMC 产品安全漏洞

EMC RSA Archer GRC 是一款治理、风险与合规的管理软件。EMC Documentum D2 是企业文档管理解决方案。EMC Documentum Content Server 是美国易安信(EMC) 公司的一套内容管理服务系统。该系统主要用于管理 Documentum 内容存储库，可对文档进行创建、修改和跟踪等操作。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、提升权限或执行任意脚本代码。

CNVD 收录的相关漏洞包括：EMC RSA Archer GRC 存在未明权限提升漏洞、EMC Documentum D2 远程权限提升漏洞、EMC Documentum Content Server 远程代码执行漏洞、EMC RSA Archer GRC Platform 跨站请求伪造漏洞、EMC RSA Archer GRC 存在未明信息泄露漏洞、EMC RSA Archer GRC 存在未明远程代码执行漏洞、EMC Documentum Content Server 信息泄露漏洞（CNVD-2014-05137）、EMC Documentum Content Server 查询注入漏洞。其中“EMC RSA Archer GRC 存在未明权限提升漏洞、EMC Documentum D2 远程权限提升漏洞、EMC Documentum Content Server 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-2014-05136>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05135>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05131>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05164>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05146>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05145>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05137>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05133>

3、WordPress 产品安全漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台，该平台支持在 PHP 和 MySQL 的服务器上架设个人博客网站。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或执行任意脚本代码。

CNVD 收录的相关漏洞包括：WordPress GB Gallery Slideshow 插件 'wp-admin/admin-ajax.php' SQL 注入漏洞、WordPress Cakifo theme 跨站脚本漏洞、WordPress 插件 All in One SEO Pack 'wp-admin/post.php' HTML 注入漏洞、WordPress 插件 Mobiloud 存在多个未明跨站脚本漏洞、WordPress 插件 Mobile Pack 'content.php'信息泄露漏洞、WordPress WP Content Source Control 插件'download.php'目录遍历漏洞、WordPress 插

件 WP Ultimate CSV Importer 存在未明漏洞、WordPress 插件 EnvialoSimple 存在多个跨站脚本漏洞。其中“WordPress GB Gallery Slideshow 插件 'wp-admin/admin-ajax.php' SQL 注入漏洞”的综合评级为“高危”。目前，除“WordPress GB Gallery Slideshow 插件 'wp-admin/admin-ajax.php' SQL 注入漏洞、Wordpress 插件 All in One SEO Pack 'wp-admin/post.php' HTML 注入漏洞、WordPress WP Content Source Control 插件'download.php'目录遍历漏洞”外，厂商已经发布其余漏洞的修补程序。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-2014-05098>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05144>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05161>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05152>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05166>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05128>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05087>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05072>

4、Apache 产品安全漏洞

Apache Axis 是 Apache web services/SOAP/WDSL 引擎，它是 Apache SOAP 项目的延续。Apache OFBiz 是一款开源的自动化项目系统。HttpComponents 简称 HttpCore，是一组底层 Http 传输协议组件，支持两种 I/O 模型，阻塞 I/O 模型和非阻塞 I/O 模型。Subversion 是一款开源多用户版本控制系统，支持非 ASCII 文本和二进制数据。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得敏感信息、进行跨站脚本攻击或执行任意脚本代码。

CNVD 收录的相关漏洞包括：Apache Axis Incomplete Fix SSL 证书验证安全绕过漏洞、Apache OFBiz 存在多个跨站脚本漏洞、Apache HttpComponents Incomplete Fix SSL 证书验证安全绕过漏洞（CNVD-2014-05105、CNVD-2014-05104）、Apache Subversion 证书验证信息泄露漏洞。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-2014-05169>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05134>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05105>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05104>

<http://www.cnvd.org.cn/flaw/show/CNVD-2014-05068>

5、BSS BS-Client SQL 注入漏洞

BSS 是业务支撑系统。本周，BSS-Client 被披露存在综合评级为“高危”的 SQL 注入漏洞。攻击者可利用漏洞提交特制的 SQL 查询，操作或获取数据库数据。目前，

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-2014-05115>

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-2014-05067	Cacti 存在未明漏洞	高	用户可以联系供应商获得补丁信息: http://cacti.net/
CNVD-2014-05061	ZPanel 存在多个 SQL 注入漏洞	高	暂无
CNVD-2014-05058	Miraj Media 'news-detail.php'nid 参数 SQL 注入漏洞	高	暂无
CNVD-2014-05057	Miraj Media 'page.php' PGID 参数 SQL 注入漏洞	高	暂无
CNVD-2014-05056	Miraj Media 'products.php' SQL 注入漏洞	高	暂无
CNVD-2014-05089	Siemens SIMATIC S7-1500 拒绝服务漏洞 (CNVD-2014-05089)	高	用户可以联系供应商获得补丁信息: http://www.siemens.com
CNVD-2014-05078	ATutor /mods/_core/courses/users/create_course.php PHP3 扩展文件上传远程代码执行漏洞	高	暂无
CNVD-2014-05099	AlienVault OSSIM 存在多个远程代码执行漏洞 (CNVD-2014-05099)	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://forums.alienvault.com/discussion/2690/security-advisory-alienvault-v4-7-0-addresses-several-vulnerabilities
CNVD-2014-05103	FFmpeg 'libavcodec/proresenc_kostya.c'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://ffmpeg.mplayerhq.hu/
CNVD-2014-05100	FFmpeg 'libavcodec/iff.c'内存破坏漏洞	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.ffmpeg.org/

表 3 部分高危漏洞列表

小结：本周，IBM 多款产品被披露存在多个漏洞，允许攻击者利用漏洞获取敏感信息、执行未授权操作或发起拒绝服务攻击。此外，EMC、WordPress、Apache 多款产品被披露存在多个漏洞，攻击者利用漏洞获取敏感信息、进行跨站脚本攻击、执行未授权操作或发起拒绝服务攻击。另外，BBS-Client 被披露存在一个高危零日漏洞。攻击者可利用漏洞提交特制的 SQL 查询，操作或获取数据库数据。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、Red Hat 修补多款产品漏洞

Red Hat JBoss Enterprise Application Platform (EAP) 是美国红帽 (Red Hat) 公司的一套开源、基于 J2EE 的中间件平台。该平台主要用于构建、部署和托管 Java 应用程序与服务。Red Hat CloudForms 是红帽子推出的混合云管理软件。

本周，Red Hat 修补了上述产品存在的安全绕过漏洞，避免攻击者可利用漏洞绕过安全限制执行未授权操作。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/49218>
<http://www.cnvd.org.cn/patchInfo/show/48910>

本周要闻速递

1. iPhone 爆安全漏洞：可自动打电话

来自 Airtame 公司的开发者 Andrei Neculaesei 最近发现了苹果 iPhone 的一个安全漏洞，可以在未经允许或不知情的情况下拨打昂贵的电话。一般当在 iOS 设备上点击一个电话号码链接的时候，设备会提示是否想拨打此电话，但是如果是使用一个本地的应用的话，系统就不会给出提示而直接拨打出去。例如，当在 Facebook Messenger 中点击一个电话号码链接的时候电话就会直接拨打出去，然而 Neculaesei 使用 Javascript 可以让设备自动点击该链接，因此最终的结果就是该电话在你不知情的情况下就拨打出去了。

参考链接：<http://news.cnfol.com/it/20140824/18770346.shtml>

2. Google Play 主流免费应用存在安全漏洞

FireEye，一家移动安全研究公司日前发布了对 Google Play 商城前 1000 免费应用的安全性研究报告，发现当中绝大多数存在 SSL/TLS 加密方面的安全漏洞。经过分析，1000 个榜单靠前的免费应用中，只有 614 个使用了 SSL/TLS 加密。614 个应用中

共有 448 个（73%）未检查加密的证书版本；1000 个应用中有 285 个实用 WebKit，当中有 219 个（77%）忽略当中产生的 SSL 错误。

参考链接：<http://tech2ipo.com/83501>

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