

信息安全漏洞周报

2016 年 10 月 17 日-2016 年 10 月 23 日

2016 年第 43 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**高**。

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 468 个，其中高危漏洞 239 个、中危漏洞 210 个、低危漏洞 19 个。漏洞平均分为 7.00。本周收录的漏洞中，涉及 0day 漏洞 97 个（占 21%）。其中互联网上出现“Linux kernel 本地权限提升漏洞（CNVD-2016-09532）、Wordpress filedownload 插件 SQL 注入漏洞”等零日代码攻击漏洞，请使用相关产品的用户注意加强防范。此外，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 1015 个，与上周（768 个）环比下降 40%。

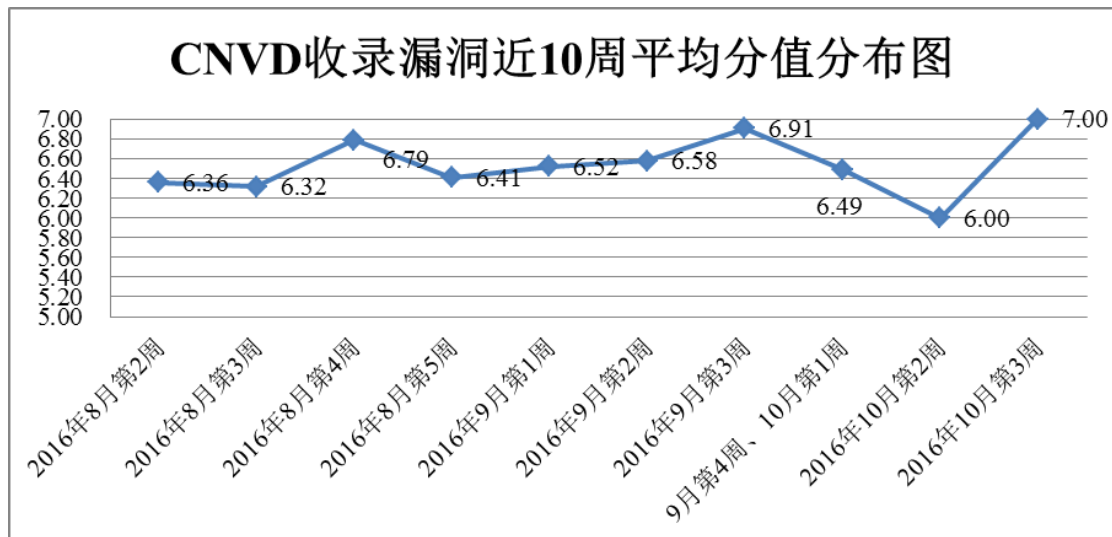


图 1 CNVD 收录漏洞近 10 周平均分分布图

本周漏洞报送情况统计

本周，共 13 家成员单位、合作伙伴及企业用户、个人用户报送了本周收录的全部 468 个漏洞。报送情况如表 1 所示。其中，东软、安天实验室、恒安嘉新、天融信、启明

星辰等单位报送数量较多。奇虎（补天平台）、漏洞盒子、中国科学院软件研究所-总体部、深圳市深信服电子科技有限公司、广西鑫瀚科技有限公司、广州神月信息技术有限公司、新疆天山智汇信息科技有限公司、南京铤迅信息技术股份有限公司及其他个人白帽子向 CNVD 提交了 1015 个以事件型漏洞为主的原创漏洞。

报送单位或个人	漏洞报送数量	原创漏洞数量
奇虎（补天平台）	801	801
东软	243	1
安天实验室	223	0
恒安嘉新	161	0
天融信	147	0
启明星辰	131	0
杭州安恒信息技术有限公司	106	26
绿盟科技	96	0
H3C	88	1
蓝盾信息技术有限公司	88	1
中国电信集团系统集成有限责任公司	20	0
卫士通信息产业股份有限公司	12	12
知道创宇	1	0
漏洞盒子	115	115
中国科学院软件研究所-总体部	7	7
深圳市深信服电子科技有限公司	6	6
广西鑫瀚科技有限公司	5	5
广州神月信息技术有限公司	3	3
新疆天山智汇信息科技有限公司	1	1

南京铨迅信息技术股份有限公司	1	1
CNCERT 山西分中心	11	11
CNCERT 福建分中心	2	2
个人	22	22
报送总计	2290	1015
录入总计	468（去重）	1015

表 1 漏洞报送情况统计表



本周漏洞按类型和厂商统计

本周，CNVD 收录了 468 个漏洞。其中应用程序漏洞 244 个，操作系统漏洞 98 个，web 应用漏洞 96 个，网络设备漏洞 21 个，安全产品漏洞 5 个，数据库漏洞 4 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	244
操作系统漏洞	98
web 应用漏洞	96
网络设备漏洞	21
安全产品漏洞	5
数据库漏洞	4

表 2 漏洞按影响类型统计表

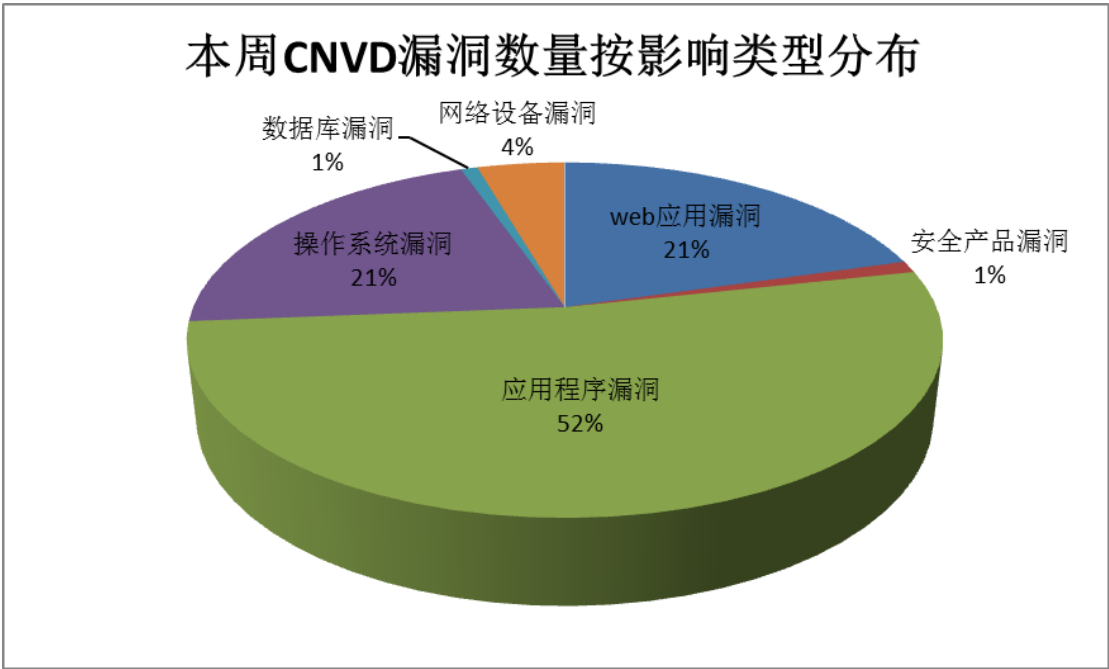


图 2 本周漏洞按影响类型分布

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

序号	厂商（产品）	漏洞数量	所占比例
1	Adobe	84	18%
2	Google	66	14%
3	Wordpress	44	9%
4	Microsoft	28	6%
5	Oracle	19	4%
6	Cisco	19	4%
7	Linux	15	3%
8	IBM	14	3%
9	SAP	6	1%
10	其他	173	38%

表 3 漏洞产品涉及厂商分布统计表

本周行业漏洞收录情况

本周，CNVD 收录了 25 个电信行业漏洞，69 个移动互联网行业漏洞，4 个工控系统行业漏洞（如下图所示）。其中，“Android 指纹登陆功能存在漏洞、Android 内核声卡驱动拒绝服务漏洞、Android Zygote 权限提升漏洞、Android Telephony 条件竞争权限提升漏洞、Android Synaptics 触屏驱动程序权限获取漏洞、Android Synaptics 触屏驱动程序权限获取漏洞、Android ServiceManager 权限提升漏洞、Android NVIDIA 摄像头驱动程序权限获取漏洞、Android Camera 权限提升漏洞（CNVD-2016-09553）、Android Camera 权限提升漏洞”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/>

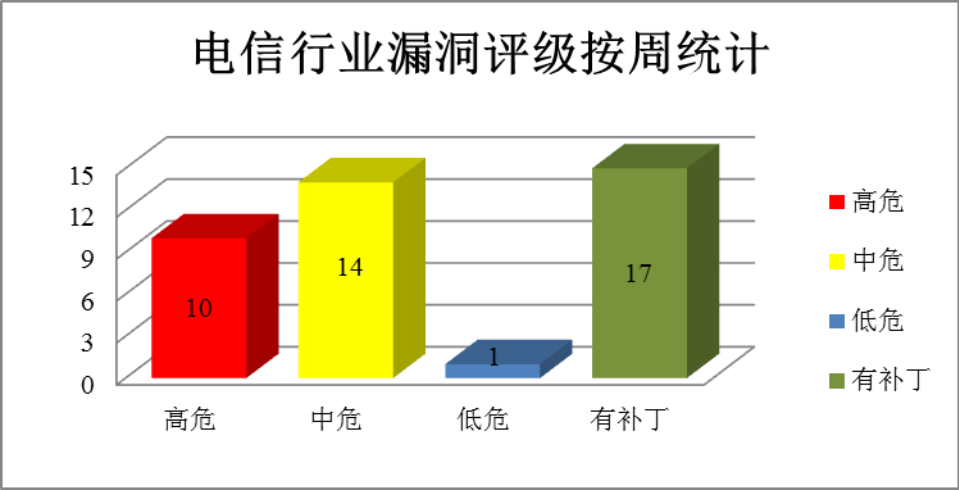


图 3 电信行业漏洞统计

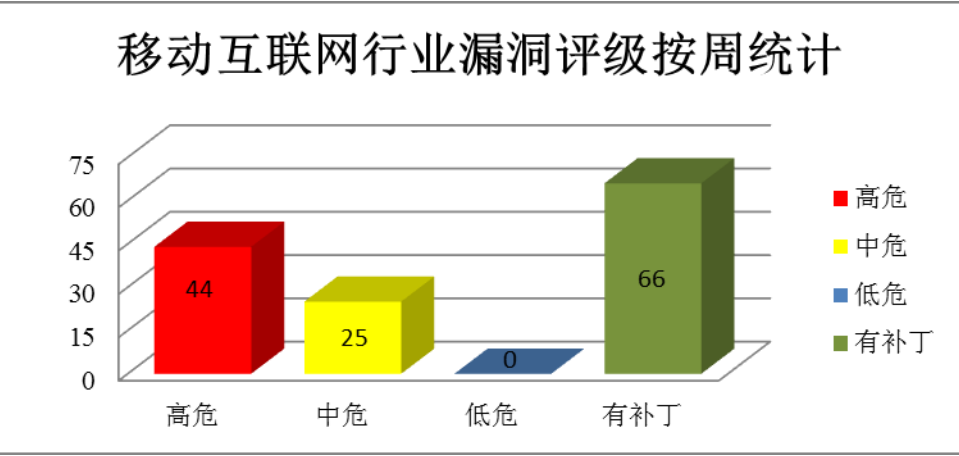


图 4 移动互联网行业漏洞统计

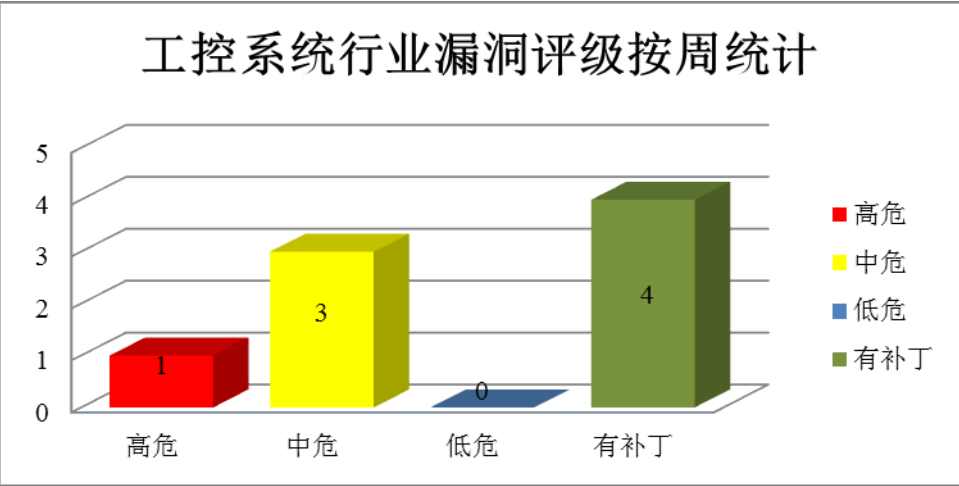


图 5 工控系统行业漏洞统计

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、Oracle 产品安全漏洞

10月19日，Oracle发布了2016年10月份的安全更新，修复了其多款产品存在的253个安全漏洞。受影响的产品包括Oracle数据库（9个）、Oracle Secure Backup数据库安全备份（2个）、Oracle Big Data Graph大数据产品（1个）、中间件产品Fusion Middleware（29个）；企业管理器网格控制产品Oracle Enterprise Manager Grid Control（5个）、电子商务套装软件OracleE-Business Suite（21个）、供应链套装软件Oracle Supply Chain Products Suite（19个）、OracleSiebel托管型CRM软件（3个）；PeopleSoft产品（11个）、JD Edwards产品（2个）、Primavera产品（2个）、Communications Applications（36个）、Financial Services Applications（24个）、HealthSciences Applications（1个）、Hospitality Applications（3个）、Insurance Applications（1个）、Retail Applications（10个）、Virtualization（13个）、Commerce（7个）Java SE（7个）、Oracle Sun系统产品（16个）和MySQL数据库（31个）。本次安全更新提供了针对116个高危漏洞的补丁，有211个漏洞可被远程利用。

CNVD收录的相关漏洞包括：Oracle Java SE组件存在未明漏洞（CNVD-2016-09702）、Oracle Java SE组件存在未明漏洞、Oracle Financial Services Applications FLEXCUBE Universal Banking组件存在未明漏洞（CNVD-2016-09684）、Oracle Financial Services Applications FLEXCUBE Universal Banking组件存在未明漏洞、Oracle Supply Chain Products Suite Agile Engineering Data Management组件存在未明漏洞、Oracle Supply Chain Products Suite Agile PLM组件存在未明漏洞（CNVD-2016-09699、CNVD-2016-09690、CNVD-2016-09691）等。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/webinfo/show/3950>

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，上述产品被披露内存破坏漏洞，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 Reader和Acrobat内存破坏漏洞（CNVD-2016-09397、CNVD-2016-09395、CNVD-2016-09394、CNVD-2016-09393、CNVD-2016-09392、CNVD-2016-09430、CNVD-2016-09431、CNVD-2016-09432）等。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-2016-09397>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09395>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09394>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09393>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09392>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09430>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09431>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09432>

3、Google 产品安全漏洞

Android 是一套以 Linux 为基础的开源操作系统。本周，该产品被披露存在权限提升和拒绝服务漏洞，攻击者可利用漏洞提升权限或发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Android Qualcomm Wi-Fi 驱动程序权限提升漏洞、Android Qualcomm 组件权限提升漏洞（CNVD-2016-09563、CNVD-2016-09574、CNVD-2016-09573）、Android Qualcomm QDSP6v2 驱动程序拒绝服务漏洞、Android Qualcomm QDSP6v2 驱动程序拒绝服务漏洞（CNVD-2016-09481、CNVD-2016-09482、CNVD-2016-09483）等。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-2016-09647>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09563>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09574>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09573>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09480>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09481>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09482>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09483>

4、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，该产品被披露存在跨站脚本漏洞，攻击者可利用漏洞进行跨站脚本攻击。

CNVD 收录的相关漏洞包括：Wordpress enhanced-tooltipglossary 插件跨站脚本漏洞、Wordpress forget-about-shortcode-buttons 插件跨站脚本漏洞、Wordpress infusionsoft 插件跨站脚本漏洞、Wordpress page-layout-builder 插件跨站脚本漏洞、Wordpress parsifont 插件跨站脚本漏洞、Wordpress simplified-content 插件跨站脚本漏洞、Wordpress whizz 插件跨站脚本漏洞、Wordpress wpsolr-search-engine 插件跨站脚本漏洞等。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-2016-09344>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09345>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09351>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09353>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09354>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09031>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09035>

<http://www.cnvd.org.cn/flaw/show/CNVD-2016-09036>

5、Joomla Ja-K2-Filter-And-Search 组件存在 SQL 注入漏洞

Joomla 是一套基于 PHP 的开源内容管理系统(CMS)。本周，Joomla 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞获取数据库敏感信息。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-2016-09609>

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-2016-09020	Fastspot BigTree CMS SQL 注入漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： https://www.bigtreecms.org
CNVD-2016-09019	多款 Panda 产品存在权限提升漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://www.pandasecurity.com/uk/support/card?id=100053
CNVD-2016-09018	Kagao 存在多个漏洞	高	用户可参考如下厂商提供的安全补丁以修复该漏洞： http://kogaoscript.com/
CNVD-2016-09009	Joomla! Huge-IT Catalog 扩展 SQL 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： http://huge-it.com/joomla-catalog/
CNVD-2016-09008	Joomla! Huge-IT Portfolio Gallery 插件 SQL 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： http://huge-it.com/joomla-portfolio-gallery/
CNVD-2016-09337	Microsoft Windows 内核 Win32k 权限提升漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://technet.microsoft.com/security/bulletin/MS16-123
CNVD-2016-09366	Microsoft Windows Graphics 远程权限提升漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://technet.microsoft.com/security/bulletin/MS16-123

			y/bulletin/MS16-120
CNVD-2016-09364	Microsoft Office 内存破坏漏洞 (CNVD-2016-09364)	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://technet.microsoft.com/security/bulletin/MS16-121
CNVD-2016-09368	Microsoft Transaction Manager 权限提升漏洞	高	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://technet.microsoft.com/security/bulletin/MS16-123

表 4 部分重要高危漏洞列表

10 月 19 日，Oracle 发布了 2016 年 10 月份的安全更新，修复了其多款产品存在的 253 个安全漏洞。本次安全更新提供了针对 116 个高危漏洞的补丁，有 211 个漏洞可被远程利用。此外，Adobe、Google、Wordpress 等多款产品被披露存在多个安全漏洞，攻击者可利用漏洞提升权限、发起拒绝服务攻击或执行未授权操作等。另外，Joomla 被披露存在 SQL 注入漏洞。攻击者可利用该漏洞获取数据库敏感信息。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. Linux 内核 9 年高龄的“脏牛”0day 漏洞

Linux 内核的内存子系统在处理写入时复制（copy-on-write, COW）时产生了竞争条件（race condition）。恶意用户可利用此漏洞，来获取高权限，对只读内存映射进行写访问。竞争条件，指的是任务执行顺序异常，可导致应用崩溃，或令攻击者有机可乘，进一步执行其他代码。利用这一漏洞，攻击者可在其目标系统提升权限，甚至可能获得 root 权限。进行 Linux 内核维护的 Greg Kroah-Hartman 宣布针对 Linux 4.8、4.7 和 4.4 LTS 内核系列的维护更新（更新后为 Linux kernel 4.8.3、4.7.9 和 4.4.26 LTS），修复了该漏洞。

参考链接：<http://www.freebuf.com/vuls/117331.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：010-82990999