国家信息安全漏洞共享平台(CNVD)

信息安全漏洞周报

2017 年 05 月 01 日-2017 年 05 月 07 日　　2017 年第 19 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 283 个，其中高危漏洞 118 个、中危漏洞 148 个、低危漏洞 17 个。漏洞平均分值为 6.18。本周收录的漏洞中，涉及 0day 漏洞 51 个（占 18%），其中互联网上出现“Joomla MyPortfolio 组件 SQL 注入漏洞、WordPress KittyCatfish 插件 SQL 注入漏洞”零日代码攻击漏洞。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 617 个，与上周（751 个）环比下降 18%。

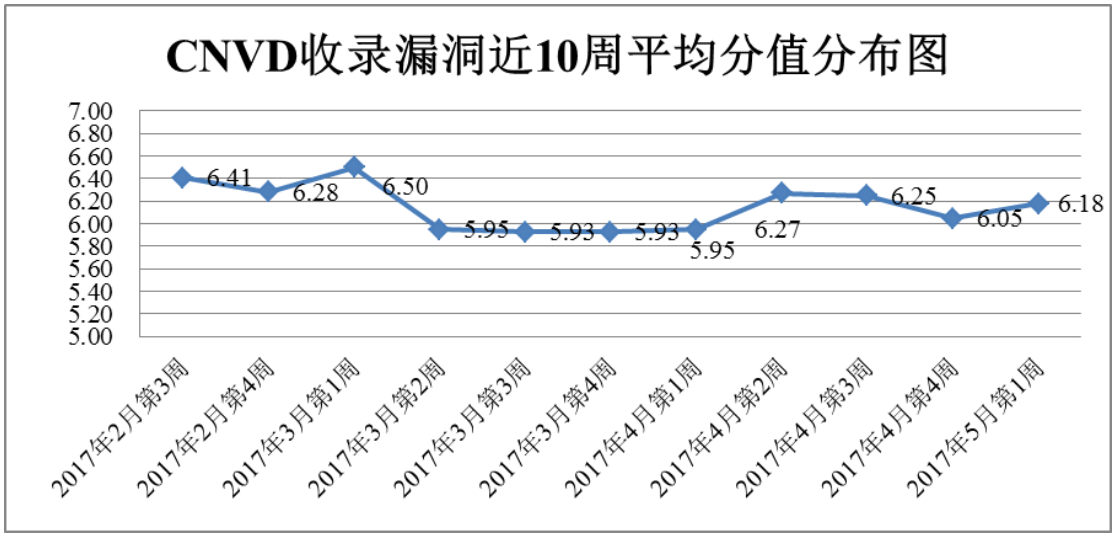

图 1 CNVD 收录漏洞近 10 周平均分值分布图

本周漏洞报送情况统计

本周，共 17 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 283 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、华为技术有限公司等单位报送数量较多。广州市网迅信息技术有限公司、山石网科通信技术有限公司、江苏君立华域信息安全技术有限公司、江西安服信息产业有限公司、山东安云信息

技术有限公司、杭州朔方信息技术有限公司、安徽新华博信息技术股份有限公司、上海观安信息技术有限公司、广州神月信息安全技术有限公司、北京安码科技有限公司及其他个人白帽子向 CNVD 提交了 617 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
360 网神	328	328
安天实验室	138	0
启明星辰	112	0
天融信	95	0
华为技术有限公司	70	1
H3C	59	0
绿盟科技	58	0
杭州安恒信息技术有限公司	34	0
中国电信集团系统集成有限责任公司	33	0
厦门服云信息科技有限公司	17	0
恒安嘉新	12	1
广西鑫瀚科技有限公司	4	4
北京知道创宇信息技术有限公司	4	3
北京无声信息技术有限公司	2	0
西安四叶草信息技术有限公司	2	2
阿里云计算有限公司	1	1
南京铱迅信息技术股份有限公司	1	1
漏洞盒子	144	144
山石网科通信技术有限公司	11	11
江苏君立华域信息安全技术有限公司	3	3

江西安服信息产业有限公司	3	3
山东安云信息技术有限公司	2	2
杭州朔方信息技术有限公司	2	2
安徽新华博信息技术股份有限公司	2	2
上海观安信息技术有限公司	1	1
广州神月信息安全技术有限公司	1	1
北京安码科技有限公司	1	1
CNCERT 海南分中心	7	7
CNCERT 北京分中心	6	6
CNCERT 湖南分中心	6	6
CNCERT 吉林分中心	6	6
CNCERT 新疆分中心	3	3
CNCERT 陕西分中心	1	1
CNCERT 河北分中心	1	1
个人	76	76
报送总计	1246	617
录入总计	283（去重）	617

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 283 个漏洞。其中应用程序漏洞 138 个，操作系统漏洞 59 个，web 应用漏洞 53 个，网络设备漏洞 20 个，数据库漏洞 10 个，安全产品漏洞 3 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	138
操作系统漏洞	59
web 应用漏洞	53

网络设备漏洞	20
数据库漏洞	10
安全产品漏洞	3

表 2 漏洞按影响类型统计表

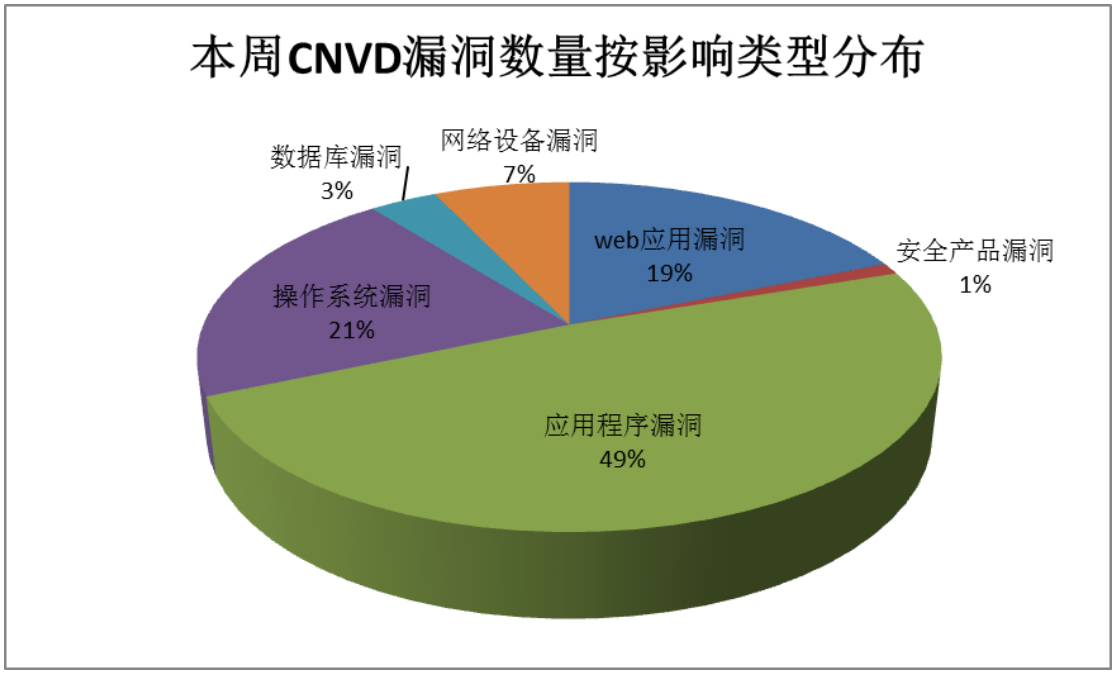

图 2 本周漏洞按影响类型分布

CNVD 整理和发布的漏洞涉及 Oracle、Microsoft、Google 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	Oracle	52	18%
2	Microsoft	29	10%
3	Google	20	7%
4	IBM	12	4%
5	Linux	12	4%
6	Vmware	9	3%
7	Huawei	7	3%
8	Apache	6	3%
9	杭州海康威视数字技术股份有限公司	5	2%
10	其他	131	46%

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 8 个电信行业漏洞，20 个移动互联网行业漏洞，1 个工控系统行业漏洞（如下图所示）。其中，“Netgear WNR2000\R2000 系列产品缓冲区溢出漏洞、Huawei Mate 9 camerafs 驱动程序缓冲区溢出漏洞、Google Android libnl 权限提升漏洞、Google Android kernel ION 子系统权限提升漏洞、mrlg4php 代码注入漏洞、Google Android HTC touchscreen driver 权限提升漏洞”等的综合评级为“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/

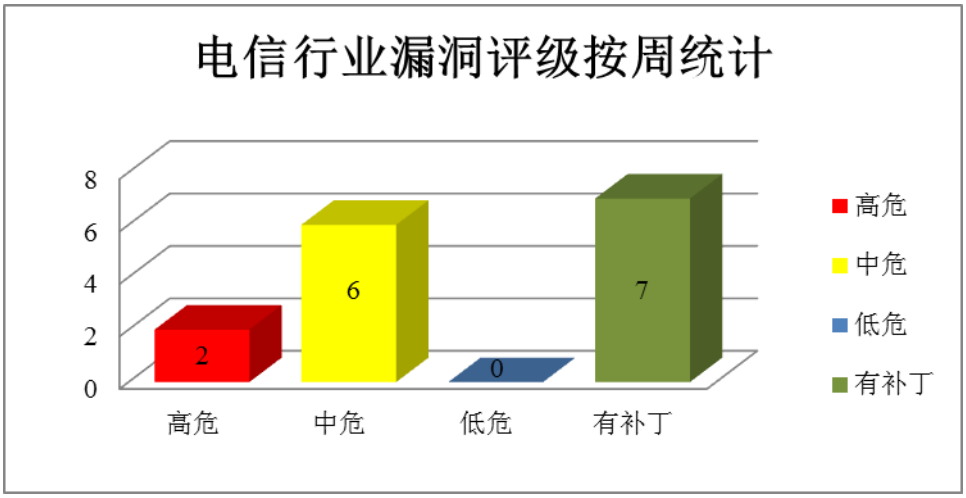

图 3 电信行业漏洞统计

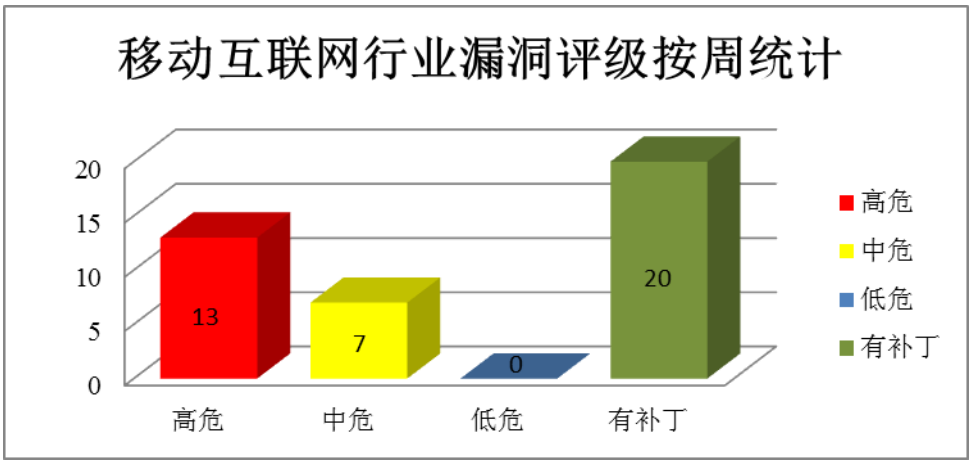

图 4 移动互联网行业漏洞统计

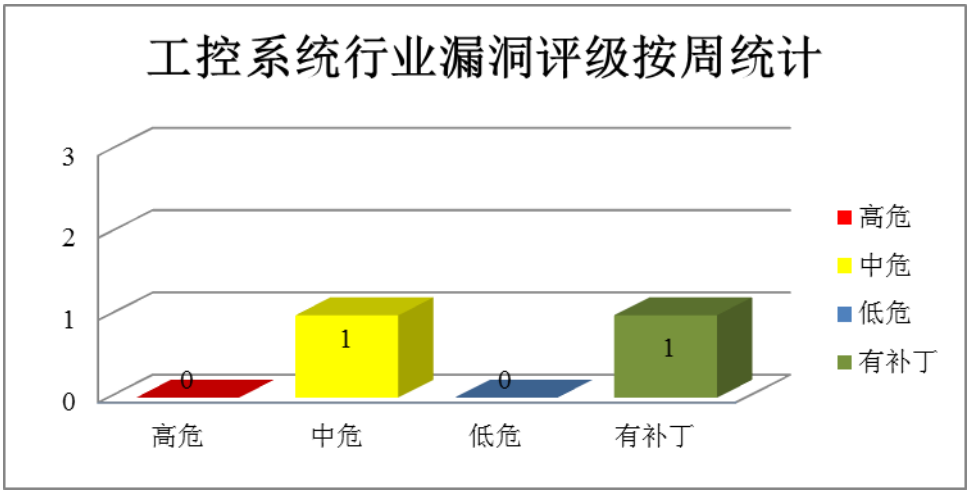

图 5 工控系统行业漏洞统计

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

Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。Oracle WebCenter Sites 是其中的一个 Web 体验管理组件。本周，该产品被披露存在远程漏洞，攻击者可利用漏洞影响机密性、完整性、可用性。

CNVD 收录的相关漏洞包括：Oracle WebCenter Sites 远程漏洞（CNVD-2017-05983、CNVD-2017-05984、CNVD-2017-05985、CNVD-2017-05986、CNVD-2017-05987、CNVD-2017-05988、CNVD-2017-05989、CNVD-2017-06025）。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-2017-05983
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05984
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05985
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05986
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05987
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05988
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05989
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06025

2、Microsoft 产品安全漏洞

Microsoft Edge 是内置于 Windows 10 版本中的网页浏览器。Internet Explorer 是微软公司推出的一款网页浏览器。Microsoft Windows 是流行的计算机操作系统。本周，

上述产品被披露存在内存破坏和远程代码执行漏洞，攻击者可利用漏洞执行任意代码。

CNVD 收录的相关漏洞包括：Microsoft Edge 脚本引擎远程内存破坏漏洞（CNVD-2017-05767、CNVD-2017-05768）、Microsoft Edge 远程内存破坏漏洞（CNVD-2017-05769）、Microsoft Internet Explorer VBScript 引擎远程内存破坏漏洞、Microsoft Internet Explorer 远程内存破坏漏洞（CNVD-2017-05771）、Microsoft Windows Hyper-V 远程代码执行漏洞（CNVD-2017-05755、CNVD-2017-05756、CNVD-2017-05757）。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-2017-05767
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05768
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05769
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05819
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05771
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05755
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05756
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05757

3、Google 产品安全漏洞

Google Android 是一款基于 Linux 开放性内核的手机操作系统。gRPC 是一个开源 RPC 框架。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：Google Android Mediaserver 拒绝服务漏洞（CNVD-2017-05710、CNVD-2017-05711、CNVD-2017-05712、CNVD-2017-05713）、Google Android Mediaserver 代码执行漏洞（CNVD-2017-05699）、Google gRPC 堆缓冲区溢出漏洞、Google gRPC 堆缓冲区溢出漏洞（CNVD-2017-06015）、Google Android NVIDIA Crypto Driver 权限提升漏洞。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-2017-05710
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05711
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05712
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05713
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05699
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06016
http://www.cnvd.org.cn/flaw/show/CNVD-2017-06015
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05725

4、Linux 产品安全漏洞

Linux kernel 是美国 Linux 基金会发布的操作系统 Linux 所使用的内核。本周，该产品被披露存在拒绝服务漏洞，攻击者可利用漏洞发起拒绝服务攻击。

CNVD 收录的相关漏洞包括：Linux kernel 拒绝服务漏洞（CNVD-2017-05860、CNVD-2017-05861、CNVD-2017-05874、CNVD-2017-05875、CNVD-2017-05876、CNVD-2017-05877、CNVD-2017-05878、CNVD-2017-05879）。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-2017-05860
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05861
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05874
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05875
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05876
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05877
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05878
http://www.cnvd.org.cn/flaw/show/CNVD-2017-05879

5、WordPress KittyCatfish 插件 SQL 注入漏洞

WordPress 是 WordPress 软件基金会的一套使用 PHP 语言开发的博客平台。本周，WordPress 被披露存在 SQL 注入漏洞，攻击者利用该漏洞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-2017-05690

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-2017-05686	IBM API Connect 命令执行漏洞	高	用户可联系供应商获得补丁信息：https://www.ibm.com/
CNVD-2017-05681	FFmpeg 堆缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息：https://www.ffmpeg.com/
CNVD-2017-05694	GE Multilin SR 继电保护器未授权访问漏洞	高	用户可联系供应商获得补丁信息：https://ics-cert.us-cert.gov/advisories/ICSA-17-117-01
CNVD-2017-05698	Dell iDRAC6 任意命令执行漏洞	高	用户可联系供应商获得补丁信息：https://www.dell.com/
CNVD-2017-05899	Tenable Appliance 任意命令执行漏洞	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.tenable.com/security/tns-2

			017-07
CNVD-2017-05955	IBM Lotus Domino 服务器堆栈缓冲区溢出漏洞	高	用户可联系供应商获得补丁信息：http://www-03.ibm.com/software/products/en/ibmdomino
CNVD-2017-05959	AlienVault OSSIM 和 USM 远程命令执行漏洞	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：https://www.alienvault.com/
CNVD-2017-05975	Apache Log4j 远程执行代码漏洞	高	用户可联系供应商获得补丁信息：https://www.apache.com/
CNVD-2017-06029	Apache Traffic Server 拒绝服务漏洞（CNVD-2017-06029）	高	用户可参考如下厂商提供的安全补丁以修复该漏洞：https://issues.apache.org/jira/browse/TS-5019
CNVD-2017-06059	TeamPass SQL 注入漏洞（CNVD-2017-06059）	高	厂商已发布了漏洞修复程序，请及时关注更新：https://github.com/nilsteampassnet/TeamPass/pull/1140

表 4 部分重要高危漏洞列表

小结：本周，Oracle 被披露存在远程漏洞，攻击者可利用漏洞影响机密性、完整性、可用性。此外，Microsoft、Google、Linux 等多款产品被披露存在多个漏洞，攻击者利用漏洞可执行任意代码、提升权限或发起拒绝服务攻击等。另外，WordPress 被披露存在 SQL 注入漏洞，攻击者利用该漏洞访问或修改数据库数据。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. WordPress 曝未经授权的密码重置漏洞

WordPress 是一个以 PHP 和 MySQL 为平台的自由开源的博客软件和内容管理系统。WordPress 的重置密码功能存在漏洞，在某些情况下不需要使用之前的身份令牌验证获取密码重置链接。该攻击可导致攻击者在未经授权的情况下获取用户 Wordpress 后台管理权限。

参考链接：http://www.freebuf.com/vuls/133816.html

2. Intel 产品系统的远程控制提权漏洞

英特尔（Intel）公司官方公布了一个严重高危（Critical）级别安全漏洞，据 Intel 声称，该漏洞主要存在英特尔管理引擎（ME)的主动管理（AMT）、服务器管理组件（ISM）、以及英特尔小企业技术（SBT）中，攻击者可以利用该漏洞进行 Intel 产品系统的远程控制提权。漏洞影响所有 Intel 企业版服务器和综合利用技术，涉及版本号为 6.x、7.x、8.x、9.x、10.x、11.5、以及 11.6 系列的所有固件产品，基于 Intel 硬件的普通个人电脑 PC 不受影响。这意味着 Intel 近十年来的固件芯片都会受到影响。

参考链接：http://www.freebuf.com/news/133657.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