

信息安全漏洞周报

2013 年 07 月 15 日-2013 年 07 月 21 日

2013 年第 29 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**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 213 个，其中高危漏洞 62 个、中危漏洞 140 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 194 个。本周收录的漏洞中，已有 181 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“McAfee ePolicy Orchestrator 存在多个漏洞”、“Advanced User Tagging Module for vBulletin 'usertag.php' 跨站脚本漏洞”等的零日攻击代码，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 5 家成员单位及个人报送了本周收录的全部 213 个漏洞。各单位报送情况如表 1 所示。其中，启明星辰、天融信、安天实验室等单位报送数量较多。此外，知道创宇公司、High-TechBridge Security Research Lab、天讯瑞达通信技术有限公司和奇虎公司以及个人报送者向 CNVD 提交了 78 个原创漏洞。其中，白帽子（ID: ccbx2000）提交了数十个受 Apache Struts 2 远程代码执行漏洞（CNVD-2013-28972，对应 CVE-2013-2251）影响的国内政府、高校和企事业单位网站漏洞事件。

报送单位或个人	漏洞报送数量	原创漏洞数量
启明星辰	180	0
绿盟科技	39	0
安天实验室	112	0
天融信	121	0

恒安嘉新	27	0
知道创宇	3	2
东软	3	0
天讯瑞达通信技术有限公司	7	1
High-Tech Bridge	1	1
奇虎 360	1	1
个人	73	73
报送总计	567	78
录入总计	213（去重）	78

表 1 成员单位上报漏洞统计表

CNVD 整理和发布的漏洞涉及 Oracle、Cisco、Google 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	Oracle	75	35%
2	Cisco	23	11%
3	Google	16	8%
4	FFmpeg	10	5%
5	Juniper	6	3%
6	Moodle	4	2%
7	HP	3	1%
8	Linux	3	1%
9	Apache	3	1%
10	Huawei	2	1%
11	其它	68	32%

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 213 个漏洞。其中应用程序漏洞 137 个，WEB 应用漏洞 19 个，操作系统漏洞 21 个，数据库漏洞 26，网络设备漏洞 10 个。

漏洞影响对象类型	漏洞数量
应用程序漏洞	137
WEB 应用漏洞	19

网络设备漏洞	10
操作系统漏洞	21
安全产品漏洞	0
数据库漏洞	26

表 3 漏洞按影响类型统计表

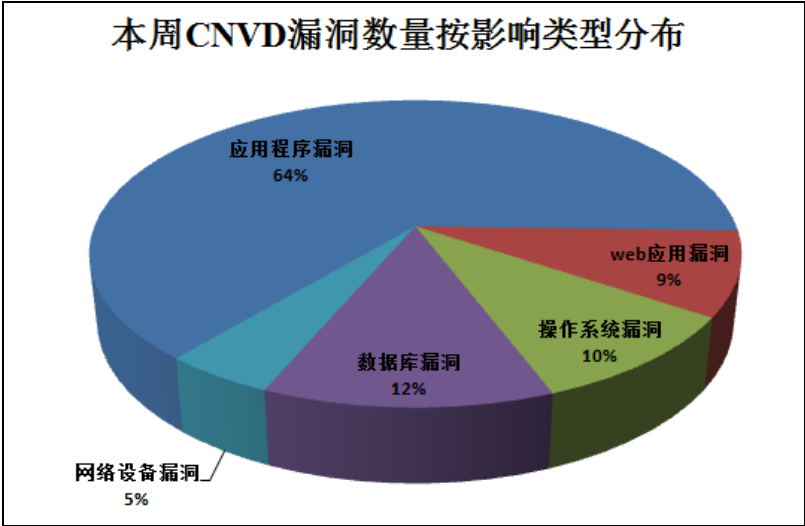


图 1 本周漏洞按影响类型分布

本周涉及电信行业漏洞信息

本周，CNVD 收录了 25 个电信行业漏洞和 1 个移动互联网行业漏洞（如下列表所示）。其中，“Oracle MySQL Server 远程拒绝服务漏洞”和“Google Android 'APK'代码远程安全绕过漏洞”的漏洞综合评级均为“高危”。相关厂商已经发布了漏洞修复程序。本周，CNVD 未收录工业系统行业漏洞。

行业	漏洞编号	漏洞标题	危险等级	是否有补丁
电信	CNVD-2013-28559	Cisco Unified Communications Management 产品跨站脚本漏洞	中危	有补丁
电信	CNVD-2013-28940	Oracle MySQL Server 远程拒绝服务漏洞	高危	有补丁
电信	CNVD-2013-28949	Cisco Secure Access Control System 帮助索引页跨站脚本漏洞	中危	有补丁
电信	CNVD-2013-28950	Cisco Secure Access Control System 管理页跨站脚本漏洞	中危	有补丁
电信	CNVD-2013-28951	Cisco Secure Access Control System 跨站脚本漏洞	中危	有补丁
电信	CNVD-2013-28952	Cisco Secure Access Control System 管理和查看页跨站请求伪造漏洞	中危	有补丁
电信	CNVD-2013-29230	Cisco Identity Services Engine Software 跨站请求伪造漏洞	中危	有补丁

电信	CNVD-2013-29237	Cisco Unified Communications Manager SQL 注入漏洞	中危	有补丁
电信	CNVD-2013-29238	Cisco Unified Communications Manager SQL 注入漏洞	中危	有补丁
电信	CNVD-2013-29239	Cisco Unified Communications Manager 本地权限提升漏洞	中危	有补丁
电信	CNVD-2013-29240	Cisco Unified Communications Manager 本地权限提升漏洞	中危	有补丁
电信	CNVD-2013-29270	Cisco Secure Access Control System 信息泄露漏洞	中危	有补丁
电信	CNVD-2013-29024	Oracle MySQL Server Server Options 子件存在未明漏洞 (CNVD-2013-29024)	中危	有补丁
电信	CNVD-2013-29025	Oracle MySQL Server Server Options 子件存在未明漏洞 (CNVD-2013-29025)	中危	有补丁
电信	CNVD-2013-29026	Oracle MySQL Server Server Parser 子件存在未明漏洞	中危	有补丁
电信	CNVD-2013-29027	Oracle MySQL Server Server Partition 子件存在未明漏洞	中危	有补丁
电信	CNVD-2013-29028	Oracle MySQL Server Server Privileges 子件存在未明漏洞	中危	有补丁
电信	CNVD-2013-29029	Oracle MySQL Server InnoDB 子件存在未明漏洞 (CNVD-2013-29029)	低危	有补丁
电信	CNVD-2013-29030	Oracle MySQL Server Server Replication 子件存在未明漏洞	低危	有补丁
电信	CNVD-2013-29031	Oracle MySQL Server XA Transactions 子件存在未明漏洞	低危	有补丁
电信	CNVD-2013-29032	Oracle MySQL Server MemCached 子件存在未明漏洞	中危	有补丁
电信	CNVD-2013-29034	Oracle MySQL Server Data Manipulation Language 子件存在未明漏洞	中危	有补丁
电信	CNVD-2013-29035	Oracle MySQL Server Full Text Search 子件存在未明漏洞	中危	有补丁
电信	CNVD-2013-29036	Oracle MySQL Server InnoDB 子件存在未明漏洞 (CNVD-2013-29036)	中危	有补丁
电信	CNVD-2013-29037	Oracle MySQL Server Prepared Statements 子件存在未明漏洞	中危	有补丁
移动互联网	CNVD-2013-28546	Google Android 'APK'代码远程安全绕过漏洞	高危	有补丁

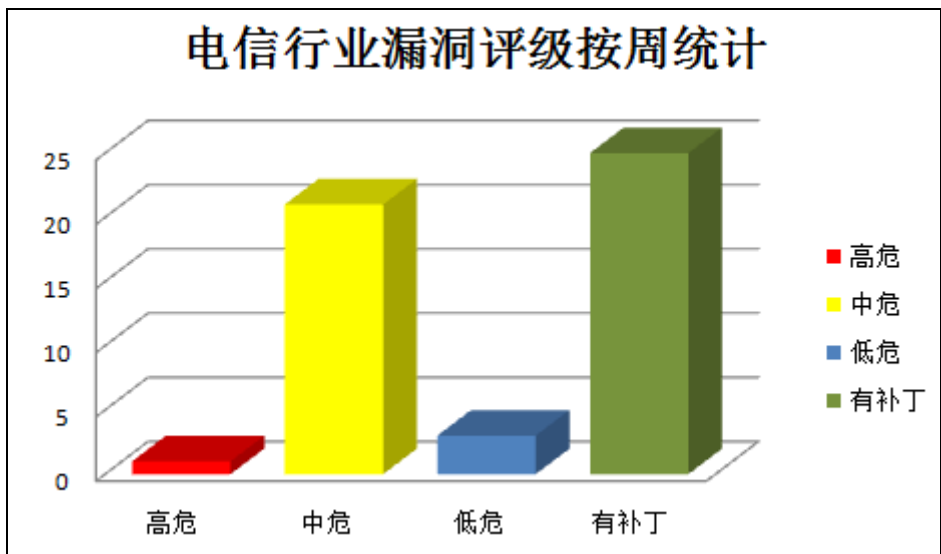


图 2 电信行业漏洞统计

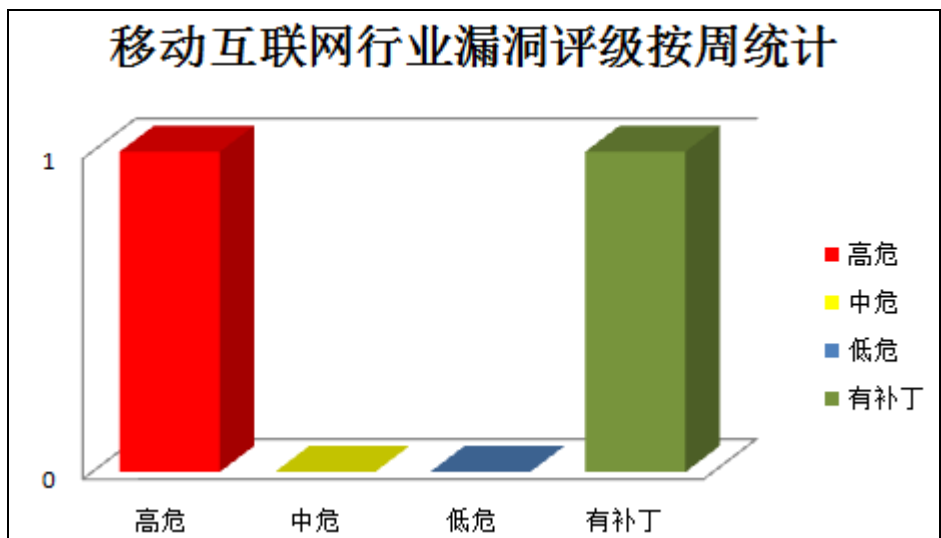


图 3 移动互联网行业漏洞统计

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、Apache Struts2 远程命令执行漏洞

Struts2 是第二代基于 Model-View-Controller (MVC)模型的 java 企业级 web 应用框架。它是 WebWork 和 Struts 社区合并后的产物。本周，Struts2 被披露存在远程命令执行漏洞和开放重定向漏洞（编号：CNVD-2013-28972，对应 CVE-2013-2251；CNVD-2013-28979，对应 CVE-2013-2248）。攻击者可以利用漏洞执行任意代码，取得服务器远程控制权。

CNVD 收录的漏洞包括：Apache Struts 远程命令执行漏洞、Apache Struts 开放重定向漏洞。上述漏洞的综合评级均为“高危”。厂商已发布上述漏洞的修补程序。CNVD

提醒广大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-2013-28979>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28972>

2、Oracle 产品安全漏洞

Oracle Solaris 是一款基于 Unix 的操作系统；Oracle Database 是一款商业性质的大型数据库；Oracle Secure Global Desktop 是 Oracle 从 Sun 获得的三个桌面虚拟化产品之一，供用户访问服务器托管的应用程序和服务器托管的桌面。本周，上述产品被披露存在安全漏洞，攻击者利用漏洞可提升权限，使应用程序崩溃或执行任意代码。

CNVD 收录的相关漏洞包括：Oracle Solaris Kernel/STREAMS framework 子件存在未明远程拒绝服务漏洞、Oracle Solaris Cluster Zone Cluster Infrastructure 子件未明本地权限提升漏洞、Oracle Solaris Cluster HA for TimesTen 子件存在未明本地权限提升漏洞、Oracle Solaris Kernel/VM 子件存在未明本地权限提升漏洞、Oracle Solaris Driver/IDM 子件存在未明远程拒绝服务漏洞、Oracle Secure Global Desktop Web UI 存在未明远程漏洞、Oracle Database Server Network Layer 组件存在未明远程代码执行漏洞、Oracle Database Oracle Executable 组件存在未明本地权限提升漏洞（CNVD-2013-28996）等。上述漏洞的综合评级均为“高危”。厂商已发布上述漏洞的修补程序。CNVD 提醒广大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-2013-29063>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29059>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29058>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29057>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29056>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29055>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28999>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28996>

3、Cisco 产品安全漏洞

Cisco Unified Communications Manager 是一款 Cisco IP 电话解决方案中的呼叫处理组件；Cisco IDSM-2 是入侵检测和防御(IDS/IPS)解决方案系列的一个组件；思科入侵预防系统(Cisco IPS)是一部能够监视网络或网络设备的网络资料传输行为的计算机网络安全设备；Cisco Secure ACS 是一款 Cisco 网络设备的中央管理平台，用于控制设备的认证和授权。本周，上述思科产品被披露存在安全漏洞，攻击者利用漏洞可使设备重载，导致拒绝服务攻击，劫持用户会话，获取敏感信息。

CNVD 收录的相关漏洞包括：Cisco Unified Communications Manager 内置加密密钥漏洞、Cisco IDSM-2 畸形 TCP 报文远程拒绝服务漏洞、Cisco IPS NME 畸形 IP 报文远程拒绝服务漏洞、Cisco IPS 畸形 IP 报文远程拒绝服务漏洞、Cisco IPS 分片通信远程拒

绝服务漏洞、Cisco Secure Access Control System 跨站脚本漏洞、Cisco Secure Access Control System 管理页跨站脚本漏洞、Cisco Secure Access Control System 帮助索引页跨站脚本漏洞等。其中，除“Cisco Secure Access Control System 跨站脚本漏洞、Cisco Secure Access Control System 管理页跨站脚本漏洞、Cisco Secure Access Control System 帮助索引页跨站脚本漏洞”外，其余漏洞的综合评级均为“高危”。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-2013-29241>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29234>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29233>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29232>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29231>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28951>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28950>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28949>

4、Juniper Junos 安全漏洞

Juniper Networks JUNOS 是一款 Juniper 网络公司的系列边界路由器等所运行的操作系统。本周，该产品被披露存在多个安全漏洞。攻击者利用漏洞可使系统崩溃导致拒绝服务攻击。

CNVD 收录的相关漏洞包括：Juniper Junos flowd 拒绝服务漏洞(CNVD-2013-28665、CNVD-2013-28664)、Juniper Junos 内核拒绝服务漏洞、Juniper Junos flowd 缓冲区溢出漏洞。上述漏洞的综合评级为“高危”。厂商已发布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-2013-28665>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28664>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28663>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28662>

5、Linux 产品安全漏洞

Linux Kernel 是一款开源的操作系统。本周，该产品被披露存在多个漏洞。攻击者利用漏洞可使系统崩溃导致拒绝服务攻击。

CNVD 收录的相关漏洞包括：kernel package-358.11.1.el6 on Red Hat Enterprise Linux 6 拒绝服务漏洞、Linux Kernel 内存错误引用漏洞（CNVD-2013-29189）、Linux fib6_add_rt2node RA 消息处理拒绝服务漏洞。其中，“Linux fib6_add_rt2node RA 消息处理拒绝服务漏洞”的综合评级为“高危”。厂商已发布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-2013-29282>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-29189>

<http://www.cnvd.org.cn/flaw/show/CNVD-2013-28919>

6、Advanced User Tagging Module for vBulletin 'usertag.php' 跨站脚本漏洞

vBulletin 是一款论坛程序。本周，该产品被披露存在一个跨站脚本漏洞。Advanced User Tagging Module for vBulletin 'usertag.php' 未能正确过滤用户提交给 hash tag 的输入，远程攻击者利用漏洞可注入恶意脚本或 HTML 代码，当恶意数据被查看时可获取敏感信息或劫持用户会话。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-2013-28654>

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-2013-29248	OpenSSH 远程拒绝服务漏洞	高	暂无
CNVD-2013-29246	多个 EMC Avamar 产品未授权访问漏洞	高	EMC Avamar Server 和 EMC Avamar Virtual Edition 7.0 已经修复此漏洞，建议用户下载更新： http://www.emc.com/products/detail/software/avamar.htm
CNVD-2013-29245	Light Audio Mixer '.wav' 文件远程拒绝服务漏洞	高	暂无
CNVD-2013-29244	Kate's Video Toolkit '.wav' 文件远程拒绝服务漏洞	高	暂无
CNVD-2013-29243	IBM AIX 多个本地权限提升漏洞	高	用户可联系厂商获得相应的升级或补丁程序： http://aix.software.ibm.com/aix/efixes/security/infiniband_advisory.asc
CNVD-2013-29229	Autodesk AutoCAD DWG 文件处理任意代码执行漏洞	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://usa.autodesk.com/adsk/servlet/ps/dl/item?id=21972896&linkID=9240618&siteID=123112
CNVD-2013-29202	WordPress Spicy Blogroll 插件 'spicy-blogroll-ajax.php' 远程文件包含漏洞	高	暂无
CNVD-2013-29195	ReadyMedia (MiniDLNA) TiVo 命令处理 SQL 注入漏洞 (CNVD-2013-29195)	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://sourceforge.net/projects/minidlna/f

			iles/minidlna/1.1.0/
CNVD-2013-29187	JGroups 'DiagnosticsHandler::run()' 报文处理安全绕过漏洞	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.jgroups.org
CNVD-2013-29185	Huawei E587 3G Mobile Hotspot /api/device/time 远程命令执行漏洞（CNVD-2013-29185）	高	暂无

表 3 部分高危漏洞列表

小结：CNVD 收录了 Apache Struts 存在一个远程命令执行漏洞和一个开放重定向漏洞（编号：CNVD-2013-28972，对应 CVE-2013-2251；CNVD-2013-28979，对应 CVE-2013-2248）。利用漏洞，可发起远程攻击，轻则窃取网站数据信息，严重的可取得网站服务器控制权，构成信息泄露和运行安全威胁。

Oracle 和 Cisco 多款产品被披露存在多个漏洞，攻击者利用漏洞可提升权限，使设备重载，执行任意代码。Juniper Networks JUNOS 和 Linux Kernel 操作系统被披露存在的漏洞可导致系统崩溃造成拒绝服务攻击。此外，vBulletin 论坛程序被披露存在一个跨站脚本的零日漏洞，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、Apache 发布升级程序，修补 Struts 安全漏洞

Apache Struts 框架是一个基于 Java Servlets,JavaBeans 和 JavaServer Pages (JSP)的 Web 应用框架的开源项目。本周，Apache 发布升级程序，修补了 Struts 框架是存在的重定向和远程命令执行漏洞。远程攻击者可以利用漏洞重定向 URL 到任意位置，或提交特殊 URL 可用于执行任意 Java 代码。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/35188>

<http://www.cnvd.org.cn/patchInfo/show/35183>

本周要闻速递

1. 部分 SIM 卡被曝存安全漏洞

7 月 22 日消息，据国外媒体报道，一安全研究人员发现部分移动 SIM 卡所使用的加密方式存在一个安全漏洞，可能会导致手机被黑客远程控制。该漏洞涉及使用 DES

数据加密标准的 SIM 卡——DES 是一种较旧的标准，目前正被部分厂商逐步淘汰，但仍有数亿张 SIM 卡使用。

参考链接：<http://tech.163.com/13/0722/07/94CDL194000915BE.html>

2. Struts2 爆高危漏洞殃及大量网站

7 月 17 日知名安全漏洞报告平台乌云发布安全警告，近期 struts 框架再次发布高危安全漏洞补丁，乌云收到众多安全厂商关于此漏洞的安全报告，此漏洞影响 struts2.0-struts2.3 所有版本，可直接导致服务器被远程控制从而引起数据泄漏，提醒各大网站和站长第一时间发现和处理安全问题处理请关注。最新的消息显示淘宝、京东、腾讯等大型互联网厂商存在该漏洞，目前影响厂商仍在增长中。而且漏洞利用代码已经被强化，可直接通过浏览器的提交对服务器进行任意操作并获取敏感内容。

参考链接：<http://net.chinabyte.com/440/12667440.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